

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO



TESIS DOCTORAL

**El delito en la cibersociedad y la justicia penal
internacional**

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Jarvey Rincón Ríos

Director

Emilio Suñé Llinás

Madrid, 2015

UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO



EL DELITO EN LA CIBERSOCIEDAD
Y LA JUSTICIA PENAL INTERNACIONAL

TESIS DOCTORAL PRESENTADA POR

JARVEY RINCÓN RÍOS

DIRECTOR: DR. EMILIO SUÑÉ LLINÁS

MADRID, 2015

<i>i. Abstract</i>	10
<i>ii. Bibliography</i>	17
<i>iii. Justificación</i>	20
A) Cuestiones metodológicas	20
B) Objetivos de la tesis.....	21
C) Consideraciones finales sobre la estructura y objetivos de la presente tesis.....	23
1. CAPÍTULO PRIMERO: INFORMACIÓN, RED Y MUNDO GLOBAL	26
1.1. De la revolución industrial a la revolución tecnológica.....	26
1.2. Modernidad e información.....	28
1.3. Postmodernidad e información	30
1.4. Virtual, espacio y velocidad	38
1.5. La Sociedad de la Información y del conocimiento.....	42
1.5.1. Configuración de la cultura global y construcción de la identidad	63
1.6. Definición de la información o el dato.....	64
1.7. Desarrollo histórico del concepto de información o dato.....	68
1.8. La información como objeto del derecho.....	74
1.8.1. La información en la historia Constitucional	74
1.8.2. Las libertades y la Información en los Tratados Internacionales referentes a Derechos Humanos	82
1.8.3. La información en el ámbito del Derecho Constitucional mundial	87
1.8.4. La información en el Constitucionalismo Colombiano	94
1.8.4.1. La información en la Constitución Colombiana de 1991	95
1.8.4.1.1. Desarrollo legislativo y jurisprudencial en materia de información y datos en Colombia.....	100
1.8.5. Ley de los Servicios de la Sociedad de la Información y Comercio Electrónico. Expresión máxima de la protección a la información en España.	117
1.9. Conclusiones.....	123
2. CIBERDELITOS COMO CONDUCTA DENTRO DE LA SOCIEDAD DE LA INFORMACIÓN	125

2.1.	Introducción.....	125
2.2.	Derecho Penal Informático.....	127
2.2.1.	Clasificación.....	128
2.3.	Definición de Derecho Penal de la Empresa.....	136
2.3.1.	Posición de las empresas transnacionales del sector financiero, de telecomunicaciones y del software	142
2.3.2.	Características de la Criminalidad Empresarial	147
2.4.	CRIMINALIDAD INFORMÁTICA	148
2.4.1.	Necesidad de una Política Criminal Informática.....	153
2.5.	CIBERDELITOS	163
2.5.1.	Teoría de la conducta en el Derecho Penal.....	163
2.5.2.	Teoría del delito en el Derecho Penal	164
2.5.3.	Desarrollo histórico del Delito informático	168
2.5.4.	Concepto de delito informático	177
2.5.5.	Naturaleza de los delitos informáticos	181
2.5.6.	Bienes e intereses jurídicos protegidos en el delito informático.....	183
2.5.7.	Características de los delitos informáticos	203
2.6.	Reflexiones Sobre la Conducta en Internet y su Influencia en la Sociedad.....	216
2.6.1.	Consideraciones preliminares.....	217
2.7.	Diferentes Conductas Relacionadas con los Delitos Informáticos.....	221
3.	LEGISLACIÓN FRENTE A LOS DELITOS INFORMÁTICOS, ELECTRÓNICOS Y DE LAS TELECOMUNICACIONES EN LA CIBERSOCIEDAD.	226
3.1.	Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en la Unión Europea.....	226
3.2.	Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Estados Unidos.	229
3.3.	Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Canadá.....	230
3.4.	Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Iberoamérica.....	232
3.4.1.	Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en España.....	232

3.4.1.1. Delitos vinculados a la informática en el Derecho Penal Español.	232
3.4.1.1.1. Delincuencia vinculada a las tecnologías de la información y la comunicación	232
3.4.1.1.1.1. Delitos cometidos contra sistemas informáticos	234
3.4.1.1.1.1.1. Delitos de Daños (atentados contra la integridad de los sistemas y los datos)	234
3.4.1.1.1.1.2. Delitos de hurto y apropiación indebida y delitos de robo	238
3.4.1.1.1.1.3. Delitos de defraudación (Abuso, acceso, utilización fraudulenta de equipos informáticos)	245
3.4.1.1.1.1.4. Delitos de falsificación (falsedades informáticas)	248
3.4.1.1.2. Delitos cometidos a través de la informática contra sistemas informáticos o informaciones digitalizadas	252
3.4.1.1.2.1. Delitos de encubrimiento y revelación de secretos (accesos informáticos ilícitos, interceptación de comunicaciones, intrusismo informático)	252
3.4.1.1.2.2. Delitos contra el secreto de empresa (espionaje informático industrial)	256
3.4.1.1.3. Delitos cometidos a través de sistemas informáticos	259
3.4.1.1.3.1. Delitos de defraudación (estafas o fraudes informáticos)	259
3.4.1.1.3.2. Delitos relativos al mercado y los consumidores (facilitación o prestación ilícita de servicios restringidos)	265
3.4.1.1.3.3. Falsedades personales (adopción fraudulenta de identidad digital falsa)	267
3.4.1.1.3.4. Delitos de difusión de contenidos lesivos para intereses diversos: libertad, libertad sexual, honor, correcto funcionamiento del mercado, derechos fundamentales y libertades públicas (delitos de difusión informática: webs de contenido sexual respecto a menores, ciberterrorismo, etc.)	269
3.4.1.1.4. Delitos contra la gestión de derechos digitales	273

3.4.1.1.4.1. Delitos contra la propiedad intelectual (pirateo informático)	274
3.4.1.1.4.2. Delitos contra la propiedad industrial	276
3.4.1.2. Un ejemplo de delitos informáticos: delitos contra sistemas y datos en el Código Penal Español ¿delitos de daños?	278
3.4.2. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Colombia.....	285
3.4.2.1. LEY COLOMBIANA SOBRE DELITOS ELECTRÓNICOS “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado- denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” (Ley 1273 del 5 de enero de 2009).....	285
3.4.2.1.1. De los atentados contra la confidencialidad, la integridad y disponibilidad de los datos en los sistemas informáticos:	288
3.4.2.1.1.1. <i>Acceso abusivo a un sistema informático.</i> Artículo 269A de la Ley 599 de 2000 (Código Penal Colombiano). Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	288
3.4.2.1.1.2. <i>Obstaculización ilegítima de sistema informático o red de telecomunicación.</i> Artículo 269B de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.....	289
3.4.2.1.1.3. <i>Intercepción de datos informáticos.</i> Artículo 269C de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.....	290
3.4.2.1.1.4. <i>Daño Informático.</i> Artículo 269D de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la	

Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	291
3.4.2.1.1.5. Uso de software malicioso. Artículo 269E de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	292
3.4.2.1.1.6. Violación de datos personales. Artículo 269F de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	294
3.4.2.1.1.7. Suplantación de sitios web para capturar datos personales. Artículo 269G de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	295
3.4.2.1.1.8. Circunstancias de agravación punitiva y Circunstancias de mayor punibilidad.	297
3.4.2.1.2. De los atentados informáticos y otras infracciones	299
3.4.2.1.2.1. Hurto por medios informáticos y semejantes. Artículo 269I de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Segundo De los atentados informáticos y otras infracciones. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	299
3.4.2.1.2.2. Transferencia no consentida de activos. Artículo 269J de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Segundo De los atentados informáticos y otras infracciones. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.	300
3.4.3. Legislación frente a los delitos informáticos en Brasil	303
3.4.4. Legislación Frente a los delitos informáticos en Argentina	304
3.4.5. Legislación frente a los delitos informáticos en Bolivia	304
3.4.6. Legislación frente a los delitos informáticos en Chile	305

4. ALCANCE DE LA CONVENCIÓN DE BUDAPEST, DEL DERECHO INTERNACIONAL HUMANITARIO Y LA COMPETENCIA Y JURISDICCIÓN DE LA CORTE PENAL INTERNACIONAL FRENTE A LOS DELITOS INFORMÁTICOS ELECTRÓNICOS Y DE LAS TELECOMUNICACIONES..	305
4.1. Derecho Penal Internacional y sus fuentes	306
4.2. Las competencias del Estado. La dimensión personal de la soberanía.....	319
4.2.1. Sobre el reparto de competencias entre los Estados	319
4.1.1. Sobre la competencia personal del Estado	321
4.2. La Responsabilidad Internacional	323
4.2.1. Las normas reguladoras de la responsabilidad internacional..	324
4.3. Invocación de la responsabilidad y Aplicación coactiva del Derecho Internacional.....	325
4.4. Aplicación coactiva del Derecho Internacional.....	328
4.5. Protección internacional de los Derechos Humanos	330
4.5.1. Consideraciones generales	330
4.5.2. Universalidad e Imperatividad	331
4.5.3. Indivisibilidad e Interdependencia	336
4.6. La Corte Penal Internacional como asociación voluntaria de Estados.	340
4.6.1. Creación de la Corte Penal Internacional.....	349
4.6.2. Sistema orgánico permanente, propio e independiente.	354
4.6.3. Autonomía jurídica de la Corte Penal Internacional.	356
4.7. La Corte Penal Internacional en el marco de la creación del orden internacional en materia de mantenimiento de la Paz del siglo XXI.	361
4.7.1. Tendencias sociales recientes en el marco de la configuración de un nuevo mantenimiento de la paz y la seguridad internacionales	363
4.7.2. Jurisdicción universal de los Estados versus jurisdicción penal internacional institucionalizada.....	371
4.8. LOS TRIBUNALES ESPAÑOLES Y LAS DECISIONES DE LOS ÓRGANOS CONVENCIONALES DE DERECHOS HUMANOS EN EL ÁMBITO UNIVERSAL.	374
4.9. La interpretación por parte de la Jurisprudencia española de las decisiones de los órganos convencionales de supervisión de Derechos Humanos.	379

4.9.1.	Conclusiones.....	386
5.	APLICACIÓN DE LA JUSTICIA PENAL INTERNACIONAL FRENTE A LOS DELITOS COMETIDOS EN LA CIBERSOCIEDAD.....	388
5.1.	IMPUTACIÓN Y DERECHO PENAL INTERNACIONAL.....	388
5.1.1.	Imputación de comportamientos macrocriminales.	388
5.1.2.	Peters: primeras reflexiones sobre una imputación de crímenes colectivos.	389
5.1.3.	Jäger: imputación individual con conducta colectiva.	391
5.1.4.	Jakobs: exoneración del autor, responsabilización de los hombres de atrás o del sistema.....	399
5.1.5.	Lampe: derecho penal del sistema como complemento de la responsabilidad individual.....	403
5.1.6.	Naucke: Creación y desarrollo de una “cuarta vía de derecho penal”.	406
5.1.7.	Marxen: puntos de partida para una teoría del delito de derecho penal internacional.....	409
5.1.8.	Resumen valorativo.	412
5.2.	REPERCUSION DE LA SOCIEDAD DEL RIESGO EN EL ORDENAMIENTO JURÍDICO PENAL.....	419
5.2.1.	Derecho A La Seguridad:	419
5.3.	TEORÍA DE LOS CRÍMENES INTERNACIONALES	422
5.3.1.	LOS CRÍMENES INTERNACIONALES COMO «CRÍMENES DE LESA HUMANIDAD»	422
5.4.	TRIBUNALES PENALES INTERNACIONALIZADOS: LA ESPECIALIZACIÓN DE LA JUSTICIA PENAL.....	427
5.4.1.	Introducción.....	427
5.4.2.	La apertura de modelos de jurisdicciones penales internacionales: los tribunales <i>ad hoc</i>	430
5.4.2.1.	La internacionalización de la justicia penal.....	430
5.4.2.2.	La definición internacional de las jurisdicciones penales internacionales.	433
5.4.3.	La creación de tribunales especiales.	438
5.4.3.1.	Naturaleza de los tribunales especiales y sus competencias.	444

5.5. Reglas jurídicas identificadas para prevenir el fraude en la contratación internacional: Autocontrol, tipificación, judicialización y cooperación nacional e Internacional	445
5.6. EL DELITO UBICUO O GLOBAL, COMO DESARROLLO DEL PRINCIPIO DE UNIVERSALIDAD. OTRA SALIDA A LA DELINCUENCIA MUNDIAL ELECTRÓNICA.	458
5.6.1. El Delito Informático como motor de cambios conceptuales en el Derecho Penal.	458
5.6.1.1. Necesidad de cambios conceptuales en el Derecho Penal .	458
5.6.1.2. Uso de medios tecnológicos como agravante de los tipos penales tradicionales	462
5.6.1.3. Interpretación extensiva de los tipos penales.....	463
5.6.1.4. Diferencia entre analogía e interpretación extensiva	464
5.6.1.5. Principio territorial y personal	466
5.6.1.6. Principios supraterritoriales.....	471
5.6.1.7. Delitos globales	472
5.6.1.8. La infracción de la regla <i>non bis in idem</i> como consecuencia de la actuación contra los delitos globales.	478
5.6.1.9. Principio de Justicia Universal.....	481
6. CONCLUSIONES	486
IV. BIBLIOGRAFÍA.....	492
V. CIBERGRAFÍA.....	500

*i. **Abstract***

CRIMES IN CYBERSOCIETY AND INTERNATIONAL CRIMINAL JUSTICE

In both, modernity and Postmodernity, the role of information is key. Among others, because human life weaves and unweaves in the constant exercise of information. This is based on the language but also in the creation of symbols, signs, ideas, movements. The modern iconography, as well as postmodern, is a summary of the great cultural, economic, and philosophical movement; There the information is key. From this perspective, the postmodern society delves into the information in the following terms: the information is the basis of production and knowledge, its raw material.

This reality is intimately linked to the actually technology transformation of machine and transport. Or better still, the first and second revolution deepens with the technology. Perhaps two elements are essential in this revolution: the space-time and the reality of the virtual. The space-time relationship is the acceleration of the speed and the virtual presence of the real thing. The virtual, "in a strict sense, has little affinity with falsehood, illusion, or imaginary. The virtual is not, in any way, the opposite of the real thing but a way of being fertile and potent that it favors the processes of creation, open horizons, digging wells full sense under the superficiality of the immediate physical presence"(LEVY, P. 1999:14) ¹.

In fact, the word virtual, says Levy, "comes from the medieval latin virtualis which in turn is derived from virtus: force, power (...)" It is what there is in power but not in Act and tends to be updated (LEVY, p. 1999:17) ². The virtual is the

¹ Lévy, Pierre. (1999). *¿Qué es lo virtual?* Barcelona: Paidós Multimedia, p. 14.

²Lévy, Pierre. (1999). *¿Qué es lo virtual?* Barcelona: Paidós Multimedia p.17.

power of the event and the virtualization the immediate reality of such an act. The virtualization of reality and their modes of information are updated in her presence there. Virtualization is the dynamics, while the virtual is a way of being. Virtualization is the dynamic that updates the data (reality), which brings the presence that which is far. This paradox is that is imposed in Postmodernity, if by this we mean the update of the given, the virtual reality of. The exodus of virtuality is embedded in the postmodern reality and plays, upsets, transforms all the worlds, the work itself. "Common sense makes virtual, imperceptible, complementary of the real" (LEVY, P. 1999:20)³.

Thus, the present becomes exodus and we see this more clearly in the virtual company. *"The virtual enterprise already cannot be located accurately. Its elements are nomadic, scattered, and the relevance of its geographical position has greatly decreased"* (LEVY, p. 1999:20)⁴. The human act of work is Telepresence, telework; the massive displacement imposed the need for speed and virtualization. The virtual time-space power information and dominion over this is the most valuable raw material.

Paul Virilio reminds us that the space has been transformed; no longer exclusively physical, also is cyberspace. *"Ciber is a new continent, ciber is a supplementary reality, the Internet should reflect the society of individuals, ciber is universal, without charge and without head"* (VIRILIO p. 1998:36)⁵. This new continent, this new area of space is configured through the network; invisible, non-existent, real, cyberspace is there, and by it we travel without moving. There take place relations between humans and everything that we conducted in the immigration, now it also happens in this new continent. What we know today as technology is nothing different than the result of explorations and discoveries of the human being, their struggles to reduce the distance in

³Lévy, Pierre. (1999). *¿Qué es lo virtual?* Barcelona: Paidós Multimedia p. 20

⁴Lévy, Pierre. (1999). *¿Qué es lo virtual?* Barcelona: Paidós Multimedia p. 20

⁵ Virilio Paul. (1998). *La bomba informática*. Paris: Galilée, 1998, p. 36.

the world; speed is the *sustratum* of this new reality. The technological revolution, revolution very important by the way as it has transformed human life and even the space where it takes place, is discursive and practical ground of utmost topicality. to the point that today we are dependent on it because it has invaded our lives. The contractual relations between subjects do not escape to the technological.

The knowledge society is generating multiple and different realities. His rise was due to the intelligent transformation of capitalism, taking advantage of the power of knowledge generated by the war, the use of technology and the rationality of science, was able to create a new paradigm, where the production of capital had large-scale, less seat in the labour force and more ideas. With her man entered a new era, marked the break with modern tradition. Knowledge and technology become, quickly, the best ally of the production of wealth, generator of new stories in the relationships between men. The virtual is to historical precisely because it breaks with the track that was able to leave the man who precedes us. The virtual is today, but disappears rapidly given the magnitude of the information and the speed that is inherent.

Science, technology and knowledge are interwoven in the contemporaneity with virtualized culture practices. The reality of human beings is an eminently physical affair linked to historical narratives. The reality is transmuted and with her new cultural practices are emerging. Man leaves his anonymity upon entering a potential and virtual world. Your stay in the world is no longer regional to become planetary. The man is no longer only, to the multiple looks that accompany it. At the same time coming out of his solitude, is controlled and by this same anonymity translates into speed. Spatial motorways printed a new destination, create other modes of relationship and lead to different

ways of being. The human being lives in the society of the speed before the control.

Among the main features of the knowledge society, there is the wide circulation of information, the advantages that are the subjects of access in real time to information and knowledge; the ability to be simultaneously in multiple and different places, different options of knowing game, as well as the uniqueness in relation with the multiple. The distant approaches and the near moves, unthinkable principle in industrial, modern and traditional society. The knowledge society supported its best ally encourages new ways of knowing and genuine knowledge practices. The human being of today can form virtually, buy in the distance, enjoy services, goods and negotiate contracts with the e. The knowledge society generates, in the singular, a new relationship with knowledge, knowledge, goods and services and is a producer of new patterns of culture.

But this new human reality is not as safe as the previous. If modernity was rich for its control, the technology systems and information is by its speed. The dangers are as real as they were in the company of tradition. Hacker and viruses are the physics of a new form of crime. The first seeks to put in check the games in cyberspace; the seconds are the story of what could be termed as "computer". Virus and Hacker are the threat of the present and the future. In this order, regular attempts, control and create a cyberspace peace, has forced international subjects to adopt measures, seeking thereby to provide security to those who must live in this so-called virtual reality.

New technologies have created new behavior object of legal States regulation, when we talk about behaviors that have to do with the new technologies of information and communication, in an attempt to clarify the different prisms from which its treatment can focus as computer crime, have been numerous

classifications that have been made of them , that, fundamentally, head to distinguish, in relation to attacks both internal and external, that is, both from within and from outside the scope of the system-authorized use, already address the same against interests of the Manager of the system already against outside interests, already in its Commission by the user, already against it. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, I. 2010:160)

In an attempt to make an effective classification, the Spanish doctrine has differentiated four groups of computer crime, the first referring to one whose taxable are the computer systems themselves, the second group, that in which harmful action rests with the data, the third is that group in which computer systems are used as a means for the Commission of the punishable, and the fourth and last group is one in which are part of the behaviors that threaten computer and digital rights.

De la Mata Barranco y Hernández Díaz, Spanish authors, have identified these four groups in the following way:

1º) which covered what is crime, which aims to attack the computer systems themselves considered with impact or not in the development of activities that allow the same.

2º) that refers to crime that aims the data work with computer, already have personal, already corporate character, developed through the use of digital contexts, which is reserves which more strictly by any author characterization of computer criminal law because it is aggression against and through computer systems. As often noted, in fact the other groups do not cover but traditional crimes committed against new material objects or through new forms of conduct nucleated ones and others around the computer or cyber fact.

3°) which encompasses all the behaviors that use computer systems to facilitate the criminal action, by a third party against the owner or the beneficiary of the system, either this against a third party, who favour new forms of attack on traditional goods or at least facilitate the extension of the harm, endangerment or the proliferation of attacks on such property.

4°) Finally, which includes what is crime, which aims only to threaten the rights arising from the processes of computing innovation or certain digital rights management.

Trying to reflect the Spanish penal code response to the issue of computer crime - while there are hardly any express allusions to concepts directly linked to it-, it must refer to crimes which, in different locations of the code, can accommodate the behaviors that should be included in any of the four groups of crimes described above as does not exist in our legal text - whose successful criterion of systematization of different crimes is basically that of the legal asset affected by each one of them-, or a chapter devoted to a concept of computer crime, cybercrime, nor a list of behaviors related to this type of criminality. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, I. 2010:160)

Returning to the Doctor Suñe Llinás approaches, we can conclude that avocando the universal principle of the criminal law, it is necessary to provide legal protection to goods mentored emerging new social, economic and technological forms through a body of universal character, for which, in this particular case, we consider that the competition must lie with the International Criminal Court, in such a way that such regulation of the legal peace to the victims of computer-related crime, who have both emotional and legal security that the violation of her rights will not go unpunished, and that at the same time have the veil of protection emanating general principles of law, according to

which universal criminal policy not to pursue internationally that remain within the territorial State orbit and crimes which are defined in the scope personal protection of each State's *Ius Puniendi*.

One of the main features of the Rome Statute, however, document guide the functioning of the International Criminal Court, as stated above, it is the subsidiary of the Statute to conduct criminal before the international criminal court judge, then our research development has led us to conclude that the short-term solution involves the application of oblique or global crime theory raised by the master Suñé Llinás where the States, making use of the principle of broad interpretation of criminal law, and as a prerequisite, having legislation that establish the crime computer, electronic or telecommunications either by their nature or by the mechanism of the Commission. This taking into account and be clear at the time involving the celebration of an amendment to an international treaty, that is the solution long term for investigation, prosecution and punishment of cybercrimes.

ii. **Bibliography**

BARREIROS, L.E., LAVOPA, F., PINTO, M., RICART, L.T., TURYN, A. (2009). Las fuentes del Derecho Internacional en la Era de la globalización. Editorial Universitaria de Buenos Aires. Primera Edición.

BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

BUSTOS, J., HOMAZÁBAL, H. (2006). Lecciones de Derecho Penal Parte General. Trotta.

CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus.

DÍAZ GARCÍA, A., RINCÓN RÍOS, J., (2009). Trámite y exposición de motivos Ley 1273 de 2009. Bogotá D.C. Colombia.

FALCÓN y TELLA, F., (2004). Para una Teoría del Conocimiento. *Foro, Nueva época*, núm. 00/2004: 69-89.

MÁRQUEZ ESCOBAR, P.C., (2002). El delito Informático. Editorial Leyer. Bogotá D.C. Colombia.

PABÓN PARRA, P.A., (2002). Manual de Derecho Penal Parte general – Parte especial. 6ª Edición. Doctrina y Ley Ltda. Bogotá D.C.

PALOMINO MARTIN, J.M., (2006). Derecho Penal y Nuevas Tecnologías. Hacia un sistema informático para la aplicación del Derecho Penal. Tirant lo Blanch. Valencia, España.

PEÑA VALENZUELA, D., (2007). Responsabilidad civil en la era digital. Editorial Universidad Externado de Colombia. Bogotá D.C. Colombia.

REYNA ALFARO, L. M., (2002). Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Juristas Editores. Lima, Perú.

RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Grupo Editorial Ibáñez: Bogotá, Colombia.

RINCÓN RÍOS, J. (2011). Justicia Internacional, una alternativa válida para el Delito Electrónico. Ponencia presentada en el Foro Delito Informático En Colombia, (Evaluación necesaria a dos años de inicio). Seguridad Informática Vs Delito Febrero 23 al 25 de 2011. Cali, Colombia.

ROVIRA del CANTO, E. (2002). Delincuencia Informática y fraudes informáticos. Editorial Comares. Granada, España.

RUSCONI, M., (2009). Derecho Penal Parte General., 2ª edición. AD-HOC. Buenos Aires.

SUÑE, LLINAS. E., (2009). *Los Derechos Humanos en el Ciberespacio. La Declaración de derechos del Ciberespacio.* ACTAS DE LA II CONVENCION INTERNACIONAL DE DERECHO INFORMÁTICO. Noviembre de 2009. Madrid, España.

VELÁSQUEZ VELÁSQUEZ F., (2010). Manual de Derecho Penal, cuarta edición, ediciones jurídicas Andrés Morales, Bogotá D.C.

ZAFFARONI, E. R., ALAGIA, A., SLOKAR, A. (2002). Derecho Penal Parte General. EDIAR. Buenos Aires.

iii. Justificación

A) Cuestiones metodológicas

La Tesis Doctoral denominada “*El delito en la cibernsiedad y la justicia penal internacional*” es un trabajo que ha sido desarrollado desde el método deductivo de investigación, partiendo de preceptos generales como la información, la red y la globalización, hasta llegar a la particularidad de la aplicación de la justicia penal internacional frente a los delitos cometidos dentro de lo que hemos denominado la cibernsiedad. Para lograr su desarrollo temático la investigación ha sido dividida en cinco capítulos dentro de los cuales se desarrolla de forma amplia cada uno de los objetivos específicos de la tesis, encontramos aportes de los grandes doctrinantes del derecho informático y penal informático español y colombiano principalmente y de otras naciones que nutren el estado del arte del derecho comparado.

La presente investigación tiene un amplio punto de partida, y es que a raíz de la interacción humana a través de los medios de comunicación e información relacionados con las redes que comparten datos, se ha dado pie a un sinnúmero de nuevas conductas que afectan a esos, también nuevos, bienes jurídicos tutelados en los ordenamientos penales relacionados con la información, la intimidad y los datos, o en otras ocasiones, la utilización de los medios informáticos, electrónicos y de las telecomunicaciones se han convertido en herramientas para la comisión de los tipos penales tradicionales. Son estas situaciones, las que nos han llevado a los diferentes planteamientos y cuestionamientos que han permitido el nacimiento de esta investigación. Analizando un caso aleatorio de una conducta ilícita realizada en cualquiera de las modalidades descritas anteriormente, nos encontramos con que los sujetos activos y pasivos del delito pueden encontrarse a miles de kilómetros de distancia, no solo con culturas, idiomas y costumbres diferentes,

sino con sistemas legales y de justicia penales que pueden tornarse completamente contradictorios donde no logre realizarse una correcta persecución de la conducta que ha vulnerado los bienes jurídicos tutelados y que de esta forma pueda materializarse uno de los preceptos de reparación para la víctima.

B) Objetivos de la tesis.

La tesis doctoral “*El delito en la cibernsiedad y la justicia penal internacional*” es una investigación de tipo deductivo que cuenta con un objetivo principal y cinco objetivos específicos.

El objetivo principal consiste en “*Proponer la base de una elaboración teórica desde la dogmática penal internacional que permita discutir sobre la necesidad de incluir la investigación y juzgamiento de los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma.*” Para el desarrollo de este objetivo se ha dividido esta investigación en cinco capítulos, cada uno de ellos corresponde al desarrollo de cada objetivo específico, así el capítulo primero se ha denominado “*Información, red y mundo global*” donde encontramos las bases fundadoras de la tesis, como ha surgido y como se ha desarrollado la cibernsiedad y como la globalización ha creado nuevos bienes jurídicos que pueden resultar afectados con los delitos informáticos. En un segundo capítulo trataremos precisamente los “*Ciberdelitos como conducta en la sociedad de la información*”, en este aparte de la tesis realizaremos un detallado análisis por las teorías y concepciones dogmáticas que diferentes autores en un marco del derecho comparado han elaborado frente a los delitos informáticos, electrónicos y de las

telecomunicaciones, refiriéndonos claramente a las diferencias cuando un delito ha vulnerado a los datos y la información como bien tutelado, y cuando los medios informáticos han sido utilizados como herramienta para la comisión de un tipo penal tradicional.

Posteriormente en un capítulo tercero podremos recorrer la legislación comparada en el ámbito colombiano y español principalmente, tomando también grandes aportes de las legislaciones de diferentes naciones europeas y latinoamericanas, con el objetivo de tener un concepto global de las conductas consideradas delito dentro de los comportamientos informáticos y uso de la información, así como de sus penas y evolución legislativa.

Como paso siguiente, procedemos a la elaboración del capítulo cuarto, denominado “*Alcance de la convención de Budapest, el derecho internacional humanitario y la competencia y jurisdicción de la Corte Penal Internacional*” en este momento investigativo empezaremos a adentrarnos en las posibles soluciones para la correcta persecución, investigación y juzgamiento de los ciberdelitos en el ámbito mundial, encontrando los primeros avances para la solución a nuestro problema de investigación.

Finalmente dentro del capítulo quinto se materializaran los esfuerzos investigativos de los cuatro capítulos anteriores en este que se denomina “*Aplicación de la justicia penal Internacional frente a los delitos cometidos en la cibersociedad*” es precisamente en este aparte donde se logra concluir un método que permita la adecuada persecución, investigación y juzgamiento de los ciberdelitos, a través de un órgano de orden mundial donde los conflictos

de jurisdicción y competencia no impidan la sanción de los ilícitos cometidos alrededor del mundo.

C) Consideraciones finales sobre la estructura y objetivos de la presente tesis.

Después de realizado todo el modelo y método investigativo se puede llegar a la conclusión que avocando el principio universal del derecho penal, es necesario brindar la protección jurídica a bienes tutelados nacientes de las nuevas formas sociales, económicas y tecnológicas a través de un órgano de carácter universal, para el que, en este caso concreto, consideramos que la competencia debe recaer en la Corte Penal Internacional, de forma que dicha regulación de la tranquilidad jurídica a las víctimas de los delitos informáticos, quienes tienen la seguridad tanto emocional como jurídica de que la violación a sus derechos no será impune, y que al mismo tiempo tenga el velo de protección emanado de los principios generales del derecho, según el cual la política criminal universal no perseguirá internacionalmente delitos que se mantengan dentro de la órbita territorial de cada estado y que se definan en el ámbito de protección personal de cada lus Puniendi estatal.

Sin embargo, una de las principales características del Estatuto de Roma, documento guía del funcionamiento de la Corte Penal Internacional, como se dijo anteriormente, es el carácter subsidiario del Estatuto para el juzgamiento de conductas penales ante la Corte Penal Internacional, entonces nuestro desarrollo investigativo nos debe guiar a que la solución a corto plazo consiste en la aplicación de la teoría del delito UBICUO o global planteada por el Maestro Suñé Llinás, donde los Estados, haciendo uso del principio de

interpretación extensiva del derecho penal, y como requisito previo, teniendo una legislación que tipifique los delitos informáticos, electrónicos o de las telecomunicaciones ya sea por su naturaleza o por el mecanismo de comisión. Esto teniendo en cuenta y siendo claros en el tiempo que implica para los Estados la celebración de una modificación a un tratado internacional, que constituye la solución a largo plazo para la investigación, juzgamiento y sanción de los ciberdelitos.

Retomando entonces, la verdadera solución a largo plazo consistiría como punto de partida la modificación al Estatuto de Roma, donde los ciberdelitos o delitos universales no sean conocidos por la Corte Penal Internacional de forma subsidiaria o residual, sino que, por el contrario, por tratarse de delitos Universales, es esta instancia de Derecho Penal Internacional quien cuenta con los requisitos y calidades para adelantar su persecución, siendo este órgano quien realice su investigación, juzgamiento y sanción, desde que se tenga conocimiento de su comisión, como instancia primaria, nunca subsidiaria, donde el objetivo claro es la aplicación del *Ius Puniendi*, ya no Estatal, sino Universal.

Además se hace indispensable que los Estados que se constituyan como partes para la investigación, juzgamiento y sanción de los ciberdelitos, acuerden en una instancia inicial la tipificación de una serie de delitos como ciberdelitos, globales o universales, revistiéndolos de las características técnicas que permiten identificar cuando su comisión ha surgido a través del ciberespacio y de esta forma sobrepasa las barreras del territorio.

Dentro de los principales componentes de este Tratado de Internacional del Ciberespacio, como hemos decidido denominarlo, debe concentrarse la lucha contra la impunidad de los delitos globales o transversales en el mundo, cuyo objetivo sea el mantenimiento de la seguridad jurídica de los seres humanos,

tomando como punto de partida los Principios generales del Derecho Penal y creando circunstancias comunes a las atribuciones del Ius Puniendi de cada uno de los miembros, lo anterior so pena de que implique modificaciones dentro de la política criminal de los Estados que se hagan miembros y dentro de sus sistemas penales, de forma que la competencia territorial no se convierta en un obstáculo para que los seres humanos sean merecedores de la justicia, al contrario, que al dejar de lado el concepto anterior de territorialidad legislativa se otorgue a las víctimas (individuales o colectivas) la reivindicación de sus derechos vulnerados y de los bienes jurídicos (de nuevo individuales o colectivos) que hayan podido ser menoscabados.

1. CAPÍTULO PRIMERO: INFORMACIÓN, RED Y MUNDO GLOBAL

1.1. De la revolución industrial a la revolución tecnológica

La transformación progresiva de la sociedad occidental moderna es concomitante con los cambios operados en el sistema de producción. La Revolución Industrial introdujo, entre la segunda mitad del siglo XVIII y principios del siglo XX, un acelerado cambio en la organización del trabajo. Tres grandes rasgos definen esta importante Revolución: tecnológicos, socioeconómicos y culturales. En los primeros se pueden situar, entre otros, el uso de nuevos materiales (hierro y acero), nuevas fuentes de energía (carbón) y una nueva fuerza traducida por la máquina a vapor. Estos tres elementos incidirían en la composición socio-económica definida por la clase obrera, la clase burguesa y la del conocimiento; esta última tiene sus máximos desarrollos en el siglo XX. Así mismo, esta importante revolución transformaría las relaciones entre las personas, generaría nuevos patrones de comportamiento y modularía la relación de los individuos con la naturaleza. Nuevas composiciones urbanas y simbólicas surgen después de la primera mitad del siglo XVIII y con ellas se despliega una anatomía del poder. Michel Foucault definiría este nuevo sistema de organización del poder de la siguiente manera: “a estos métodos que permiten el control minucioso de las operaciones del cuerpo, que garantizan la sujeción constante de sus fuerzas y les imponen una relación de docilidad-utilidad es a lo que se puede llamar disciplina”⁶ (FOUCAULT, M. 2002:141). La disciplina del cuerpo está dirigida al control de la conducta humana. Los dispositivos que ella despliega pueden resumirse así: docilidad de los cuerpos, encauzamiento de la buena conducta y el sistema panóptico. Estos tres grandes dispositivos despliegan, a la vez, ciertas tipos de individualización.

⁶ FOUCAULT, Michel. (1976). *Vigilar y Castigar. Nacimiento de la prisión*. Buenos Aires: Siglo XXI editores, p. 141.

“(...) puede decirse que la disciplina fabrica, a partir de los cuerpos que controla, cuatro tipos de individualidad (...) celular (juego de la distribución espacial), orgánica (cifrado de las actividades), genética (acumulación del tiempo) y combinatoria (la composición de las fuerzas)” (FOUCAULT, M. 2002:141)⁷.

Estos tipos de individualización están acompañados de las siguientes técnicas:

“(...) construye cuadros, prescribe maniobras, impone ejercicios y dispone de tácticas. La táctica, arte de construir, con los cuerpos localizados, las actividades codificadas y las aptitudes formadas, unos aparatos donde el producto de las fuerzas diversas se encuentra aumentado por una combinación calculada” (FOUCAULT, M. 1976:141)⁸.

Esta racionalidad de la actividad humana estaría profundamente unida al trabajo del cual se desprenden las conductas y la moral capitalista. El trabajo produce riqueza y define el modo de la propiedad; el trabajo rige el tiempo pues la actividad se impone en las relaciones hombre-espacio. Mientras la campana impuso, durante varios siglos, el ritmo de las actividades humanas, el reloj las define. En el trabajo, la acción se define en tiempo cronológico y éste es inherente a la sociedad disciplinar y por esto mismo es moderno.

El trabajo es la moral del capitalismo y define los valores de propiedad cuyos efectos vemos en otras esferas de la vida. En el ejercicio del intercambio de bienes y mercancías se reafirma el poder sobre la propiedad. En el momento

⁷ FOUCAULT, Michel. (1976). *Vigilar y Castigar. Nacimiento de la prisión*. Buenos Aires: Siglo XXI editores, p. 172.

⁸ FOUCAULT, Michel. (1976). *Vigilar y Castigar. Nacimiento de la prisión*. Buenos Aires: Siglo XXI editores, p. 172.

en que este poder es socavado el quiebre de la libertad es inminente y con ello, la fractura del pacto social. El pacto social es un contrato cuyo objeto es la libertad y, el derecho, es la instancia vigilante. El derecho es la acción racional que se aplica cuando las acciones negativas resquebrajan el principio de libertad. Esto será clave, incluso en los giros de humanización del derecho y del castigo, de la pena y de la sanción (FOUCAULT, M. 1976:117)⁹.

El derecho moderno humaniza su ejercicio al superar el poder del soberano. Puesto que la sociedad disciplinar es inherente a la Revolución Francesa, un nuevo pacto político irrumpe y con ello se impone una nueva relación hombre-Ley. La libertad, adviene un fin supremo; la igualdad, un ejercicio de la soberanía y, la fraternidad, la práctica del recto derecho.

1.2. Modernidad e información

El marco filosófico en el que emergen estas dos revoluciones es, indiscutiblemente, la Ilustración y su territorio, la razón. Ella es la superación del mito y de la superstición. Las leyes que la regirían son, el juicio recto, la creencia en el poder de la ciencia, el descubrimiento y dominio sobre la naturaleza. La sociedad occidental después de la mitad del siglo XVIII y hasta mediados, aproximadamente, del siglo XX, estaría fundada en el poder de la ciencia y de la razón instrumental. La razón se despliega en la idea de lo moderno. La modernidad, desde una perspectiva clásica, es como lo sugiere Touraine, “la construcción de una imagen racionalista del mundo que integra

⁹ El suplicio, práctica de punición fuertemente aplicada antes de la mitad del siglo XVII, se transformará en la benignidad de la pena. Así, mientras el suplicio buscaba causar públicamente el mayor daño posible en el culpable, la benignidad de la pena recogería el sentimiento de ira de la sociedad a través de los tribunales. El poder judicial se hace público y se desprende de la venganza del soberano. “...para cada delito su ley, para cada criminal su pena”. FOUCAULT, Michel. (1976) p. 117

al hombre en la naturaleza, el microcosmos en el macrocosmos, y que rechaza toda forma de dualismo del cuerpo y del alma, del mundo humano y del mundo trascendente” (TOURAINÉ, A. 1994:35)¹⁰. La sociedad moderna se regirá, según Anthony Giddens, por cuatro grandes dimensiones: el industrialismo, el capitalismo, la industrialización de la guerra y la vigilancia de todos los aspectos de la vida social”¹¹.

Ahora bien, el claro desarrollo de la modernidad, la nación, la empresa y el consumidor, tal como lo sugiere Touraine, está más allá de la simple reducción de lo moderno a la razón instrumental, al cálculo y a la autoridad racional¹². Estos tres elementos delimitan el espacio. En efecto:

“(...) la nación se define más por una cultura que por una acción económica, la empresa tiende a obtener beneficios y poder así como la organización racional de la producción, los consumidores introducen con sus elecciones aspectos cada vez más diversos de su personalidad a medida que su nivel de vida les permite satisfacer necesidades menos elementales y por lo tanto menos encuadradas dentro de las reglas tradicionales” (TOURAINÉ, A. 1994:35)¹³.

Ahora bien, la modernidad como motor del pensamiento, potenciadora de las técnicas de ciencia y dinamizadora de la libertad humana, tendrá su punto de realización en el trabajo. Puesto que el trabajo es la fuente de generación de riqueza y de bienestar y también de profundas luchas, la sociedad moderna teje sus propias contradicciones. De un lado, ella cifra su poder en la

¹⁰ Touraine, Alain. (1994). *Crítica de la modernidad*. México: Fondo de Cultura Económica, p. 35.

¹¹ Giddens, Anthony. (1992). *The consequences of Modernity*. Cambridge: Polity Press, p. 38.

¹² Touraine, Alain. (1994). *Op. Cit.*, p. 135.

¹³ Touraine, Alain. (1994). *Crítica de la modernidad*. México: Fondo de Cultura Económica, p. 135.

información. La sociedad moderna inventó la prensa, el cable noticioso y la publicidad. La sociedad moderna es libre y esto se reafirma en el poder del derecho. En cuanto garantiza la posición de los individuos respecto a la información y al trabajo, la sociedad moderna instaura la libertad positiva. La sociedad moderna es abierta, profundamente desarrollista, ampliamente unificadora. Ella hace del lenguaje la práctica de la libertad. A través del lenguaje, la sociedad moderna unifica la diferencia, borra los particularismos culturales. El progreso está en la máquina y con ella se firma la superación de lo viejo. Al borrar las diferencias culturales y los particularismos lingüísticos, ella acerca lo lejano. De otro lado, la sociedad moderna, al hacer del trabajo el reino de la libertad, deviene un sistema de poder cuyo objeto es el cuerpo, su fuerza y conciencia. A la vez, esta idea de libertad, se rige por el consumo, la propiedad, el deber, las normas, el poder disciplinador. Mientras en su discurso, la modernidad libera, en la práctica somete. Por esto, la razón deviene el contra-poder del dogma y del mito. Así, en la sociedad industrial, moderna y libre, la energía del sistema tiene lugar en la relación: tiempo-trabajo.

1.3. Postmodernidad e información

A la sociedad moderna, cuya base de producción del trabajo era la transformación de las materias primas, se impondrá la sociedad postmoderna, regida, entre otras, por la predominancia del conocimiento y de la información. La noción de postmodernismo, sin discusión equívoca, surge en el curso de la década de los setenta, en la escena artística e intelectual, anunciando una nueva era del arte, el saber y la cultura, aunque como su mismo nombre lo apunta, debe ser comprendida con relación a la era que le antecede. En efecto, ella invita a un retorno prudente a nuestros orígenes, a una perspectiva histórica de nuestro tiempo, a una interpretación en profundidad de la era de

la que salimos parcialmente pero que, en muchos aspectos, prosigue su obra (LIPOVETSKY, G. 2000:79)¹⁴.

Lipovetsky, siguiendo la lectura de *Les Contradictions culturelles du capitalisme*, de Daniel Bell, se propone mostrar el postmodernismo “como una hipótesis global que describe el paso lento y complejo a un nuevo tipo de sociedad, de cultura y de individuo que nace del propio seno y en la prolongación de la era moderna” (LIPOVETSKY, G. 2000:80)¹⁵. Por ello, no lo circunscribe “a un marco regional, estético, epistemológico o cultural: si aparece una postmodernidad, ésta debe designar una ola profunda y general a la escala del todo social, puesto que es cierto que vivimos unos tiempos en que las oposiciones rígidas se borran, en que se difuminan las preponderancias, ya que la inteligencia del momento exige poner de manifiesto las correlaciones y homologías” (LIPOVETSKY, G. 2000:80)¹⁶. En esta perspectiva, se hace necesario comprender el contenido del modernismo, su genealogía y funciones históricas y seguir los cambios que paulatinamente se produjeron en el curso del siglo XX, y que conllevaron a la preeminencia de los sistemas flexibles y abiertos. (LIPOVETSKY, G. 2000:80)¹⁷.

Con relación a la cultura, lugar donde muy seguramente se da inicio al movimiento postmoderno, encontramos cómo el capitalismo, desde la primera mitad del siglo XIX, sufrió una profunda crisis cultural, denominada modernismo, cuya característica principal radica en rupturas, discontinuidades, en el culto a la novedad y al cambio. No obstante, el apogeo

¹⁴ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 79.

¹⁵ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, p. 80.

¹⁶ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, pp. 79-80.

¹⁷ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, p. 80.

de esa crisis se realiza entre 1880 y 1930, cuando la representación clásica deja su espacio hegemónico, cuando la escritura se libera de las represiones de la significación codificada y cuando surgen los grupos y artistas de vanguardia. Odio a la tradición y furor de la renovación total, marcan los rasgos de los adeptos al modernismo. Radical en sus convicciones, en su propio seno se instala la negación a la tradición: *“las obras de vanguardia, tan pronto como han sido realizadas, pasan a la retaguardia y se hunden en lo ya visto”* (LIPOVETSKY, G. 2000:81)¹⁸. Crítica, flujo, negación e invención perpetua, se convierten en contradicción inmanente al modernismo, pues, como lo señalara Octavio Paz, *“el modernismo es una especie de autodestrucción creadora... el arte moderno no es sólo hijo de la edad crítica, sino el crítico de sí mismo”*. (LIPOVETSKY, G. 2000:81)¹⁹ *“Tradición de lo nuevo” (...) el único principio que rige al arte es la propia forma del cambio”* (LIPOVETSKY, G. 2000:82)²⁰.

Hacia finales de los años treinta, sin embargo, esa contradicción dinámica del modernismo creativo da paso a una fase *“no menos contradictoria, y además fastidiosa y vacía de toda originalidad”* (LIPOVETSKY, G. 2000:82)²¹. La incapacidad de una innovación artística importante, la pérdida del poder creativo de la negación, conducen a la reproducción y plagio de los descubrimientos del primer tercio del siglo. Según Bell, es la entrada del posmodernismo, caracterizado por una doble contradicción: su objetivo es generar sin cesar algo absolutamente distinto y, sin embargo, al final sólo

¹⁸LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, p. 81.

¹⁹ Citado en: LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 81

²⁰ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, p. 82.

²¹ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,, p. 82.

“produce lo idéntico, el estereotipo, la repetición” (LIPOVETSKY, G. 2000:82)²², el no-sentido.

Si bien el posmodernismo coincide con la “*sociedad tecnificada*”, “*por sí misma evacuadora de cualquier sentido*”, ésta no determina los cambios culturales. Como lo señala D. Bell en Lipovetsky, “*el posmodernismo no es el reflejo de la sociedad posindustrial*” (LIPOVETSKY, G. 2000:83)²³, sino que es producto de la cultura modernista, profundamente individualista y radical, que erige como valor preponderante lo nuevo, la negación de cualquier orden estable (LIPOVETSKY, G. 2000:83)²⁴. La cultura individualista del modernismo se instaura a finales del siglo XIX, cuando los artistas se rebelan contra los valores de la clase burguesa, centrados en el trabajo, la moderación y el puritanismo, y recurren, inspirados en el romanticismo, a valores centrados en la exaltación del yo, la autenticidad y el placer (LIPOVETSKY, G. 2000:83)²⁵.

Las críticas contra las convenciones e instituciones sociales dominan el espacio artístico, que se diferencia del espíritu burgués con su culto al dinero, al trabajo, al ascetismo y al radicalismo. Por el contrario, teniendo por centro al yo, el modernismo es una cultura de la personalidad: “*vivir con la máxima intensidad, “desenfreno de todos los sentidos*”, seguir los propios impulsos e imaginación, abrir el campo de experiencias” (LIPOVETSKY, G. 2000:83)²⁶. El individualismo ilimitado y hedonista permeará a la tradición burguesa en los primeros años del siglo XX, a pesar de la resistencia de los burgueses frente a la cultura modernista.

²²LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 82.

²³ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama., p. 83.

²⁴ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 83.

²⁵ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama., p. 83.

²⁶ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 83.

Para Bell, el hedonismo, propio de la cultura moderna, circunscrita al modo de vida de los artistas, se extendió en Estados Unidos en la segunda década del siglo XX, como modo de vida corriente, con la aparición del consumo de masa. Este hecho, marca la gran revolución cultural de las sociedades modernas. *“Si se mira la cultura bajo la óptica del modo de vida, será el propio capitalismo y no el modernismo artístico el artesano principal de la cultura hedonista”* (LIPOVETSKY, G. 2000:84)²⁷. La moral puritana cede el paso a valores hedonistas que animan a gastar, disfrutar de la vida, ceder a los impulsos: la masificación del lujo, la publicidad, la moda, los *mass media*, y el crédito lo hicieron posible.

Según la hipótesis de Bell, se estableció así una cultura que reúne los efectos conjugados del modernismo y del consumo de masa, centrada en la realización personal, la espontaneidad y el placer, en oposición abierta a la lógica de la economía y de la política. La sociedad moderna resulta de la articulación compleja de tres órdenes distintos, con sus respectivos principios, a veces adversos, sus propios ritmos de cambio y con normas diferenciadas: el tecno-económico, el régimen político y la cultura. De la mezcla de estos órdenes dispares *“resultan las diversas contradicciones de la sociedad”* (LIPOVETSKY, G. 2000:84-85)²⁸. Para el sociólogo norteamericano, las sociedades modernas sufren una profunda crisis cultural y espiritual, gracias a las lógicas antinómicas que rigen los tres órdenes que constituyen el capitalismo moderno: el hedonismo para la cultura o formas de vida, la eficacia en el orden tecno-económico y la igualdad en la esfera del poder y la justicia social (LIPOVETSKY, G. 2000:84-85)²⁹.

²⁷LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 84.

²⁸Bell, citado por LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, pp. 84-85.

²⁹ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama,., pp. 84-85.

El modernismo, como movimiento artístico, surge como una prolongación de la institución de las sociedades democráticas:

“El modernismo no es más que un aspecto del amplio proceso secular que lleva al advenimiento de las sociedades democráticas basadas en la soberanía del individuo y del pueblo, sociedades liberadas de la sumisión a los dioses, de las jerarquías hereditarias y del poder de la tradición. Prolongación cultural del proceso que se manifestó con el esplendor en el orden político y jurídico a fines del siglo XVIII, culminación de la empresa revolucionaria democrática que constituyó una sociedad sin fundamento divino, pura expresión de la voluntad de los hombres que se reconocen iguales” (LIPOVETSKY, G. 2000:85-86)³⁰.

Por otro lado, el modernismo también es prolongación de una cultura individualista en la que se promueve un proceso de legitimación de todos los sujetos y, en este sentido, debe entenderse como la extensión de la dinámica revolucionaria (Revolución Francesa) al orden cultural (LIPOVETSKY, G. 2000:88-89)³¹, que “sólo pudo aparecer gracias a una lógica social e ideológica tan flexible que permitió la producción de contrastes, divergencias y antinomias” (LIPOVETSKY, G. 2000:93)³² y donde se exaltó, lo que Daniel Bell denomina “el eclipse de la distancia” (LIPOVETSKY, G. 2000:96)³³, que corresponde, en el orden de las artes plásticas, a la destrucción del espacio

³⁰ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 84-86

³¹ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, pp. 88-90.

³² LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 93.

³³ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 96.

escenográfico euclidiano, a la ruptura de la escena representativa que anula la distancia entre la obra y el espectador.

Al término de la fase modernista, hacia la década del sesenta, la personalización, el individualismo que la caracterizaron, con relación a las posturas de los artistas, se extiende al público en general, gracias al consumo de masas que levanta como valor central de nuestra cultura al hedonismo (LIPOVETSKY, G. 2000:105)³⁴; la democratización del hedonismo permite que los valores del modernismo se lleven al extremo a nivel cultural y político: “revuelta estudiantil, contracultura, moda de la marihuana y del L.S.D., liberación sexual, pero también películas y publicaciones porno-pop, aumento de violencia y de crueldad en los espectáculos, la cultura cotidiana incorpora la liberación, el placer y el sexo” (LIPOVETSKY, G. 2000:105-106)³⁵. Consumo y hedonismo constituyen el “epicentro del modernismo y el posmodernismo” (LIPOVETSKY, G. 2000:106)³⁶. Pero si la libertad individual es el motor de las luchas modernas y posmodernas, también el control total de la sociedad hace parte de estos movimientos:

“La revolución del consumo que no llegará a su plenitud hasta pasada la Segunda Guerra Mundial tiene, a nuestro modo de ver, un alcance mayor: reside esencialmente en la realización definitiva del objetivo secular de las sociedades modernas, es decir, el control total de la sociedad y, por otra parte, la liberación cada vez mayor de la esfera privada en manos del autoservicio generalizado, de la velocidad de la moda, de la flexibilidad de los principios, roles y estatutos. Al absorber al individuo en la carrera por el nivel de

³⁴LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 105.

³⁵ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, pp. 105-106.

³⁶ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama., p. 106.

vida, al legitimar la búsqueda de la realización personal, al acosarlo de imágenes, de informaciones, de cultura, la sociedad del bienestar ha generado una atomización o una desocialización radical, mucho mayor que la que se puso en marcha con la escolarización en el siglo XIX” (LIPOVETSKY, G. 2000:106-107)³⁷.

El posmodernismo es considerado como la era del consumo, para la que la demanda de necesidades e informaciones rompe las fronteras de lo local, arranca al individuo de su tierra natal y, más aún, de la estabilidad de la vida cotidiana, produciendo una cultura nacional e internacional. “El hombre moderno está abierto a las novedades, apto para cambiar sin resistencia de modo de vida, se ha vuelto cinético” (LIPOVETSKY, G. 2000:107)³⁸. La moda, la obsolescencia acelerada, la desustancialización, marcarán la constitución de los individuos: “emergencia de individuos aislados y vacilantes, vacíos y reciclables ante la continua variación de los modelos” (LIPOVETSKY, G. 2000:107)³⁹, expectantes frente a la imposición seductora de innovaciones que opera el consumo como mecanismo de control y de administración generalizada de lo cotidiano: “la era del consumo se inscribe en el vasto dispositivo moderno de la emancipación del individuo por una parte, y de la regulación total y microscópica de lo social por otra” (LIPOVETSKY, G. 2000:107-108)⁴⁰. Fórmula ambigua, el consumo produce un sujeto que debe hacerse cargo de sí mismo, a responsabilizarse de sus decisiones que se multiplican al verse obligado a “escoger permanentemente, a tomar iniciativas, a informarse, a criticar la calidad de los productos, a auscultarse y ponerse a prueba, a mantenerse joven, a deliberar sobre los actos más simples”

³⁷ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, pp. 106-107.

³⁸ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 107.

³⁹ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama., p. 107.

⁴⁰ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, pp. 107-108.

(LIPOVETSKY, G. 2000:109)⁴¹. Singularidad de los individuos y universalización de los modos de vida. Con relación a esto último, Lipovetsky señala que:

“Uno de los fenómenos importantes residen en que desde ahora la cultura está sometida a las normas gestionarias prevalentes en la “infraestructura”: los productos culturales han sido industrializados, sometidos a los criterios de la eficacia y de la rentabilidad, tienen las mismas campañas de promoción publicitaria y de marketing. Simultáneamente, el orden tecno-económico es inseparable de la promoción de las necesidades, y por lo tanto del hedonismo, de la moda, de las relaciones públicas y humanas, de los estudios de motivación, de la estética industrial” (LIPOVETSKY, G. 2000:127)⁴².

1.4. Virtual, espacio y velocidad

Tanto en la modernidad como en la postmodernidad, el papel de la información es clave. Entre otras, porque la vida humana se teje y desteje en el ejercicio constante de la información. Esta tiene su base en el lenguaje pero también en la creación de símbolos, señales, ideas, movimientos. La iconografía moderna, así como postmoderna, es el resumen del gran movimiento cultural, económico y filosófico; allí la información es pieza clave. Desde esta perspectiva, la sociedad postmoderna profundiza en la información en los siguientes términos: la información es la base de la producción y, el conocimiento, su materia prima. Esta realidad está

⁴¹ LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama., p. 109.

⁴² LIPOVETSKY Gilles. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama, p. 127.

íntimamente unida a la transformación de la máquina y el transporte en realidad tecnológica. O mejor aún, la primera y segunda revolución se profundiza con la tecnología. Tal vez dos elementos son esenciales en esta revolución: el espacio-tiempo y la realidad de lo virtual. La relación espacio-tiempo es la aceleración de la velocidad y lo virtual la presencia de lo real. Lo virtual, “en un sentido estricto, tiene poca afinidad con lo falso, lo ilusorio o lo imaginario. Lo virtual no es, en modo alguno, lo opuesto a lo real sino una forma de ser fecunda y potente que favorece los procesos de creación, abre horizontes, cava pozos llenos de sentido bajo la superficialidad de la presencia física inmediata” (LÉVY, P. 1999:14)⁴³. En efecto, la palabra virtual, nos dice Lévy, “procede del latín medieval *virtualis* que a su vez deriva de *virtus*: fuerza, potencia (...) es lo que existe en potencia pero no en acto y tiende a actualizarse (LÉVY, P. 1999:17)⁴⁴. Lo virtual es la potencia del acto y la virtualización la realidad inmediata de dicho acto. La virtualización de la realidad y sus modos de información se actualizan en la presencia-ahí. La virtualización es la dinámica, mientras que lo virtual es una forma de ser. La virtualización es la dinámica que actualiza el dato (realidad), que trae a la presencia aquello que está lejano. Esta paradoja es la que se impone en la postmodernidad, si por ésta entendemos la actualización de lo dado, lo virtual de su realidad. El éxodo de la virtualidad se incrusta en la realidad postmoderna y toca, trastoca, transforma todos los mundos, el trabajo mismo. “*El sentido común hace de lo virtual, imperceptible, complementario de lo real*” (LÉVY, P. 1999:20)⁴⁵. Así, lo presente se hace éxodo y esto lo vemos con mayor claridad en la empresa virtual. “*La empresa virtual ya no se puede situar con precisión. Sus elementos son nómadas, dispersos, y la pertinencia de su posición geográfica ha decrecido enormemente*” (LÉVY, P. 1999:20)⁴⁶. El acto humano del trabajo se hace tele-presencia, teletrabajo; el desplazamiento

⁴³ LÉVY, Pierre. (1999). ¿*Qué es lo virtual?* Barcelona: Paidós Multimedia, p. 14.

⁴⁴ LÉVY, Pierre. (1999). ¿*Qué es lo virtual?* Barcelona: Paidós Multimedia., p.17.

⁴⁵ LÉVY, Pierre. (1999). ¿*Qué es lo virtual?* Barcelona: Paidós Multimedia., p. 20

⁴⁶ LÉVY, Pierre. (1999). ¿*Qué es lo virtual?* Barcelona: Paidós Multimedia., p. 20

masivo impuso la necesidad de la velocidad y de la virtualización. Lo virtual del tiempo-espacio potencia a la información y el dominio sobre ésta es la materia prima más valiosa.

Paul Virilio nos recuerda que el espacio se ha transformado; ya no es exclusivamente físico, también es ciber-espacio. *“El Ciber es un nuevo continente, el ciber es una realidad suplementaria, el ciber debe reflejar la sociedad de individuos, el ciber es universal sin responsable y sin cabeza”* (VIRILIO P. 1998:36)⁴⁷. Este nuevo continente, este nuevo espacio del espacio se configura a través de la red; invisible, inexistente, real, el ciberespacio está ahí y por él transitamos sin movernos. Allí tienen lugar relaciones entre humanos y todo lo que realizábamos en el espacio-materia, ahora también acontece en este nuevo continente. Lo que hoy conocemos como tecnología no es cosa distinta que el resultado de las exploraciones y descubrimientos del ser humano, sus luchas por disminuir la distancia en el mundo; la velocidad es el *sustratum* de esta nueva realidad. La revolución tecnológica, revolución importantísima por la forma como ha transformado la vida humana, e incluso el espacio donde ella tiene lugar, es un terreno discursivo y práctico de suma actualidad. La tecnología incide en la vida humana, al punto que hoy dependemos de ella pues ha invadido nuestra vida. Las relaciones contractuales entre sujetos no escapan a lo tecnológico. Paul Virilio lo narra así:

“Privados progresivamente del uso de nuestros órganos receptores naturales, de nuestra sensualidad, estamos maravillados, como lo está el minusválido, por una especie de desmesura cósmica, la búsqueda fantasmática de mundos y modos diferentes donde el antiguo “cuerpo animal” no tendría más lugar, donde se realizaría

⁴⁷ VIRILIO, Paul. (1998). *La bomba informática*. Paris: Galilée, 1998, p. 36.

la simbiosis entre lo humano y lo tecnológico” (VIRILIO P. 1998:49)⁴⁸.

Tal como lo habíamos escrito más arriba, la revolución tecnológica tuvo su génesis en la revolución del transporte y las comunicaciones. Dicha revolución envuelve, a la vez, tres grandes revoluciones: la cibernética (VIRILIO P. 1998:13)⁴⁹, la bio-tecnológica y la cuántica. La vida humana, después del advenimiento de la tecnología, cambió radicalmente. El ser humano se ha beneficiado de los progresos evidentes de la tecnología. Sus procesos de comunicación se han acelerado, sus formas de estar en el mundo se han transformado y sus modos de realización en la vida trazan otros relatos. El ser humano vive en una totalidad mundial y, a la vez, experimenta una singular realidad. La velocidad (VIRILIO P. 1998:25)⁵⁰, nos lo recuerda Virilio, aparece como el nuevo discurso. El mundo se aclara por la velocidad y lo inmediato rompe las fronteras. La relación espacio/tiempo está determinada por la velocidad. Ella marca las relaciones de estar en el mundo; el hombre se mueve menos y viaja más rápido. La velocidad la encontramos incluso en la arquitectura. Puesto que la velocidad es *“la luz de la luz”*, el hábitat humano recoge este nuevo modo de ver. Los centros comerciales, los espacios públicos o el transporte masivo tienen como característica no ser oscuros. La velocidad del espacio es visibilidad y por esto mismo control. La velocidad, nuevamente nos lo recuerda Virilio, se transforma en un dispositivo de control. Verlo todo desde un ojo oculto es la nueva práctica de lo humano y deviene

⁴⁸ VIRILIO, Paul. (1998). *La bomba informática*. Paris: Galilée, 1998, 49.

⁴⁹ Respecto a la cibernética, él afirma que ella es una “ciencia extrema”, una tecnocultura de masas, no es el agente de la aceleración de la Historia como antes, sino el vértigo de la aceleración de la realidad y esto en detrimento de toda verdadera imagen” *Ibíd.*, p. 13.

⁵⁰ El concepto de velocidad de la velocidad es central en la revolución tecnológica. Ella rompe la relación espacio/tiempo y se muestra como el verdadero objeto de la aceleración del tiempo humano. “La velocidad no sirve únicamente para desplazarse, ella sirve ante todo para ver, entender, percibir y, en consecuencia, concebir más intensamente el mundo presente. Mañana, ella servirá para actuar a la distancia, más allá del área de influencia del cuerpo humano y de su ergonomía comportamental”. Cfr. VIRILIO Paul. (1991). *La vitesse de libération*, Paris: Galilée, p. 25.

un arma para los sistemas policivos. Todo lo vemos y a la vez somos vistos, todo lo controlamos y a la vez somos controlados. Esta nueva realidad es la expresión de la revolución tecnológica. Sus dispositivos de visibilidad cámaras, circuitos, dispositivos de comunicaciones, interfaces, internet, etc., integran la vida y la recrean a la vez. Tal vez, el poder más importante no sea lo político sino lo tecnológico; pues hasta la noción misma de hombre se ha transformado. Lo trans-humano y la miniaturización de los dispositivos de comunicación son una realidad presente que acelera el desarrollo del ser humano. En efecto, el ser humano se mueve menos pero viaja más rápido (VIRILIO P. 1998:46-47)⁵¹. La vida humana está afectada por la tecnología y con ella se han transformado los modos de relación entre individuos; el derecho no escapa a esta nueva realidad. La bioética, así como el biopoder, muestra ya un nuevo discurso; el derecho se ve afectado y debe reorientar sus formas de comprensión del hecho info-jurídico.

1.5. La Sociedad de la Información y del conocimiento

Los signos que marcan, delimitan y nombran una época determinada emergen primero de manera tímida, esporádica, como un rumor apenas esbozado y luego invaden el espacio, apareciendo en todos los lugares a veces como constatación de su existencia, otras como interrogación de ella, o se proponen y discuten formas diferentes de nombrarlo. Todos, hoy, coinciden en reconocer que nuestro tiempo es otro, diferente, al tiempo pasado. Los filósofos, los sociólogos, los psicólogos y, en general, los investigadores de la condición humana, empezaron a señalarlo desde hace tres décadas. Pero también lo señalaban los investigadores cuya preocupación se dirigía más a pensar cómo las formas de la inteligencia humana podían replicarse y, hasta

⁵¹ Virilio Paul. (1990). *La inercia polar*. Paris: Christian Bourgois éditeurs, pp.46-47.

perfeccionarse, fuera de lo humano. Algo estaba en proceso de cambio, algo estaba mutando hacia nuevas formas que determinarían la relación del hombre con el mundo – relación con las cosas del mundo, relación con los otros en el mundo y relación consigo mismo-.

Así, leemos en el inicio de Imperio, de los filósofos políticos Hardt y Negri, el anuncio de un nuevo orden de carácter mundial:

“El imperio se está materializando ante nuestro propios ojos. Durante las últimas décadas, a medida que se derrumbaban los regímenes coloniales, y luego, precipitadamente, a partir de la caída de las barreras interpuestas por los soviéticos al mercado capitalista mundial, hemos asistido a una globalización irreversible e implacable de los intercambios económicos y culturales. Junto con el mercado global y los circuitos globales de producción surgieron un nuevo orden global, una lógica y una estructura de dominio nuevas: en suma, una nueva forma de soberanía” (HARDT. M, y NEGRI. A. 2002:11)⁵².

En el mismo sentido, el anuncio del cambio lo encontramos al inicio de la trilogía del sociólogo Manuel Castells:

“Hacia el final del segundo milenio de la era cristiana, varios acontecimientos de trascendencia histórica han transformado el paisaje social de la vida humana. Una revolución tecnológica, centrada en torno a las tecnologías de la información, está modificando la base material de la sociedad a un ritmo acelerado. Las economías de todo el mundo se han hecho interdependientes

⁵² HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, p. 11.

a escala global, introduciendo una nueva forma de relación entre economía, Estado y sociedad en un sistema de geometría variable” (CASTELLS, M. 2006:27)⁵³.

Y, constatando estas transformaciones, el sociólogo Touraine, nos ofrece la siguiente descripción del tiempo actual, también al inicio de *¿Podremos vivir juntos?*, título sugerente frente a la sociedad que enfrentamos:

“Las informaciones, como los capitales y las mercancías, atraviesan las fronteras. Lo que estaba alejado se acerca y el pasado se convierte en presente. El desarrollo ya no es la serie de etapas a través de las cuales una sociedad sale del subdesarrollo, y la modernidad ya no sucede a la tradición; todo se mezcla; el espacio y el tiempo se comprimen. En vastos sectores del mundo se debilitan los controles sociales y culturales establecidos por los estados, las iglesias, las familias o las escuelas, y la frontera entre lo normal y lo patológico, lo permitido y lo prohibido, pierde su nitidez. ¿No vivimos en una sociedad mundializada, globalizada, que invade en todas partes la vida privada y pública de la mayor cantidad de personas? Por lo tanto, la pregunta planteada, “¿podemos vivir juntos?”, parece exigir en primer lugar una respuesta simple y formulada en presente: ya vivimos juntos. Miles de millones de individuos ven los mismos programas de televisión, toman las mismas bebidas, usan la misma ropa y hasta emplean, para comunicarse de un país al otro, el mismo idioma. Vemos cómo se forma una opinión pública mundial que debate en vastas asambleas internacionales, en Río o en Pekín, y que en todos los continentes se preocupa por el calentamiento del planeta, los

⁵³ CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I.* México: Siglo XXI Editores, 7ª ed., p. 27.

*efectos de las pruebas nucleares o la difusión del sida”
(TOURAINÉ, A. 2000:9)⁵⁴.*

O, también, las advertencias de Ulrich Beck:

“En todo el mundo, la sociedad contemporánea está sometida a un cambio radical que plantea un reto a la modernidad basada en la Ilustración y abre un ámbito en el que las personas eligen formas sociales y políticas nuevas e inesperadas... Todos están de acuerdo en que en las épocas venideras nos enfrentaremos a profundas contradicciones y paradojas desconcertantes, y en que experimentaremos esperanzas envueltas en desesperación” (BECK, U. 2002:1)⁵⁵.

Podríamos continuar revisando los diferentes análisis que aparecieron a finales de la década de 1990 y principios de la primera década del tercer milenio⁵⁶ y encontraremos inscrito el signo que anuncia el cambio o, mejor, la concreción de un cambio que comenzó a fraguarse en décadas anteriores. En efecto, todos coinciden en señalar que el cambio no es un acontecimiento que irrumpe sin anunciarse, por el contrario, es el resultado de un proceso que va poco a poco cristalizándose. En general, los inicios de este proceso se sitúan en el período de postguerra, en particular la década de 1950, período que

⁵⁴TOURAINÉ, Alain. (2000). *¿Podremos vivir juntos?* Bogotá: Fondo de Cultura Económica, p. 9.

⁵⁵ BECK, Ulrich. (2002). *La Sociedad del Riesgo global*. Madrid: Sigo XXI Editores, p. 1.

⁵⁶ En la década de 1970 aparecen los discursos del cambio social, denominado por algunos el paso de la sociedad industrial a la sociedad post-industrial (Alain Touraine, 1969; Daniel Bell, 1973); o de la modernidad a la posmodernidad (Lyotard, 1979). En la década de 1990 y principios de 2000 aparecen nuevos discursos que intentan mostrar el cambio que se inicia en los 70: la desmodernización (Touraine, 1997); la sociedad informacional (Castells, 1999); imperio (Hardt y Negri, 2000); la modernidad líquida (Bauman, 2000); la sociedad informacional (Castells, 1999), entre muchos otros.

preparará el terreno y que empezará su concreción en la década de 1970 con lo que se denominó la tercera revolución, o revolución tecnológica y que se extenderá a nivel global en la década de 1990.

Pero, ¿cuál es la naturaleza del cambio anunciado? ¿Cómo describen, analizan, explican y/o comprenden este cambio los diversos autores? Podrían señalarse diversas dimensiones de la vida humana que el cambio atraviesa. Así, algunos hacen mayor énfasis en la dimensión política, otros en la dimensión social, y otros en la dimensión cognitiva (ciencia y tecnología). Todas estas dimensiones se interrelacionan, pues, tal como lo anuncian los discursos, la naturaleza del cambio es global, tanto en el sentido territorial –la mundialización- como en el sentido de la experiencia de la vida humana –el control de las formas de vida y de relaciones de vida-. En el centro del cambio está, pues, la vida humana que, debe ser gobernada, administrada, controlada. Aspecto que no es nuevo pues, éste hace parte de la modernidad, cuando el hombre aparece, en el centro de ella misma, como el individuo de la vida, el lenguaje y el trabajo (FOUCAULT, M. 1966)⁵⁷. Desde la dimensión política y social, la gubernamentalidad de lo humano está determinada por las formas de producción económica. Pero estas dimensiones atravesarán también la dimensión personal, pues, para todos es conocido que, hoy, el individuo es por lo que desea y puede conseguir a través de su actividad económica. Lo económico sería, entonces, una dimensión que englobaría las otras.

Para la modernidad, lo económico jugó un papel preponderante, pues, en palabras de Bauman, con la expresión de Marx y Engels “*derretir los sólidos*”, se abrió el camino para liberar la iniciativa comercial (Max Weber) “de los grilletes de las obligaciones domésticas y de la densa trama de los deberes éticos”, en el que se derretían además “todos los vínculos que condicionan la

⁵⁷ FOUCAULT, Michel. (1966). *Las palabras y las cosas*. Madrid: Siglo XXI Editores.

reciprocidad humana y la mutua responsabilidad, conservar tan sólo el “nexo del dinero” (Thomas Carlyle). La disolución de los sólidos, afirma Bauman,

“destrababa toda la compleja trama de las relaciones sociales, dejándola desnuda, desprotegida, desarmada y expuesta, incapaz de resistirse a las reglas del juego y a los criterios de racionalidad inspirados y moldeados por el comercio, y menos capaz aun de competir con ellos de manera efectiva [...] Esa fatal desaparición dejó el campo libre a la invasión y al dominio de (como dijo Weber) la racionalidad instrumental, o (como lo articuló Marx) del rol determinante de la economía: las “bases” de la vida social infundieron a todos los otros ámbitos de la vida el status de “superestructura” –es decir, un artefacto de esas “bases” cuya única función era contribuir a su funcionamiento aceitado y constante-” (BAUMAN, Z. 2003:10)⁵⁸.

Para contribuir, de manera eficaz, al funcionamiento aceitado y constante de la vida social, cuyo valor primordial estaba centrado en la producción económica, los individuos debieron ser formados, normalizados, disciplinados, tal como lo ilustra Foucault (1975), quien denominará a estas formas de sujeción del individuo como biopolítica. Las sociedades disciplinarias se encargaron de la formación del individuo para el trabajo efectivo y para la producción cada vez más tecnificada de los productos de consumo que la sociedad industrial requería. Pero esta sociedad industrial no es la que hoy domina. En efecto, la sociedad post-industrial (Touraine, 1969; Bell, 1973) surge de esa forma de sociedad pero cambia el acento de sus intereses. Si

⁵⁸ BAUMAN, Zygmunt. (2003). *Modernidad Líquida*. Buenos Aires: Fondo de Cultura Económica, p. 10.

para la sociedad industrial, lo importante era la producción de bienes de consumo y, para ello se requería de la disciplina de los individuos formados en el modelo de la sociedad fábrica; para la sociedad post-industrial, el bien predominante lo constituye en un primer momento la información y en un segundo momento el conocimiento. Así, el bien que se produce no es exterior al hombre, por el contrario, es inmanente a él y, por ello, la producción de ese bien requiere de nuevas formas de concebir la formación de los individuos. Esa formación no consistirá propiamente en capacitar al individuo para producir bienes exteriores sino para producir un bien que está en sí mismo: el conocimiento. La biopolítica será, entonces, el redoblamiento de la producción de riqueza, como se desprende de lo que afirman Hardt y Negri:

“En la posmodernización de la economía global, la creación de riqueza tiende cada vez más hacia lo que denominamos producción biopolítica, la producción de la misma vida social, en la cual lo económico, lo político y lo cultural se superponen e infiltran crecientemente entre sí” (HARDT. M, y NEGRI. A. 2002:12-13)⁵⁹.

El paso de la sociedad industrial a la sociedad post industrial está dado por lo que se denominó la tercera revolución, o revolución de la tecnología de la información. Esta revolución fue posible gracias a los avances tecnológicos derivados, a su vez, en los avances del conocimiento, de lo que se denominó en la década de 1950 la revolución cognitiva. Los descubrimientos de la cibernética abonaron el terreno para el surgimiento, en la década de 1970, de dos herramientas que transformarían el mundo: la tecnología computacional y la interconexión en tiempo real a través de la red de comunicaciones, internet. La invención de estos dos artefactos, a decir de Castells, constituyó

⁵⁹ HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, pp. 12-13.

“Un acontecimiento histórico al menos tan importante como lo fue la Revolución Industrial del siglo XVIII, inductor de discontinuidad en la base material de la economía, la sociedad y la cultura [...] (con una) capacidad de penetración en todos los dominios de la actividad humana no como una fuente exógena de impacto, sino como el paño con el que está tejida esa actividad. En otras palabras, se orientan hacia el proceso, además de inducir nuevos productos [...] Por otra parte, a diferencia de cualquier otra revolución, el núcleo de transformación que estamos experimentando en la revolución en curso remite a las tecnologías del procesamiento de la información y de la comunicación [...] Lo que caracteriza a la revolución tecnológica actual no es el carácter central del conocimiento y la información, sino la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de la información/comunicación, en un círculo de retroalimentación acumulativo entre la innovación y sus usos” (CASTELLS, M. 2006:56-58)⁶⁰.

La revolución tecnológica abrirá el camino a lo que hoy conocemos como sociedad del conocimiento. Esta denominación resalta el papel hegemónico que el conocimiento ha adquirido. Aunque muchos coinciden en señalar que el conocimiento ha sido fundamental en la historia de la humanidad y en los cambios y revoluciones que se han producido en las diferentes etapas, hoy ha tomado un giro diferente. En efecto, el conocimiento ha estado presente en

⁶⁰ CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I*. México: Siglo XXI Editores, 7ª ed., pp. 56-58.

las sociedades desde la antigüedad, *“la historia y la antropología nos enseñan que desde la más remota antigüedad todas las sociedades han sido probablemente sociedades del conocimiento, cada una a su manera”* (UNESCO, 2005:17)⁶¹. En algunas épocas y sociedades, el conocimiento fue instrumento de exclusión, reservado para pequeñas elites quienes disponían de él de manera secreta; en otras, en particular desde el siglo de las luces, se intentó la democratización del conocimiento a partir de la difusión de las ideas que gobernaban el espíritu de la época: universalidad, libertad e igualdad. La invención de la imprenta, y la creciente producción del libro, facilitó la difusión de los conocimientos. Hoy, las nuevas formas de difusión de los conocimientos han sobrepasado el medio impreso. La internet, y con ella, la creación de las herramientas virtuales como las bibliotecas y librerías virtuales, los e-learning y universidades virtuales, los blogs o grupos de discusión, el correo electrónico, entre muchas otras, ha favorecido la distribución exponencial del conocimiento. Esta descripción rápida de la circulación del conocimiento todavía deja muchas preguntas en relación con las formas de igualdad que podría crear el acceso más equitativo de esta gran herramienta del pensamiento humano. En *Hacia las sociedades del conocimiento*, la UNESCO se pregunta si *“poseemos ya los medios que permitan un acceso igual y universal al conocimiento, así como un auténtico aprovechamiento compartido de éste”* pues para este organismo internacional, el desarrollo humano y sostenible depende de la construcción de sociedades de conocimiento auténticas (UNESCO, 2005:17)⁶².

Pero ¿a qué se alude cuando se habla de conocimiento? ¿Qué es el conocimiento? ¿Cómo éste puede llegar a dominar una sociedad determinada? Los análisis sociológicos, filosóficos y políticos señalan una dirección para responder a esta cuestión. La relación entre los modos de

⁶¹ UNESCO. (2005). *Hacia la sociedad del Conocimiento*. Paris: Unesco, p. 17.

⁶² UNESCO. (2005). *Hacia la sociedad del Conocimiento*. Paris: Unesco, p. 17.

producción de una sociedad determinada y el nivel de conocimiento que ésta ha logrado desarrollar. En el centro de esta relación aparece la categoría sociológica del trabajo. Como lo señala Castells, “el proceso del trabajo está en el núcleo de la estructura social” (CASTELLS, M. 2006:229)⁶³. El concepto de trabajo es constituyente de la condición humana moderna (BAUMAN, Z. 2003:14)⁶⁴. Una genealogía del trabajo es descrita por Foucault como sigue:

“En efecto, el trabajo – es decir, la actividad económica– sólo apareció en la historia del mundo el día que los hombres fueron demasiado numerosos para poder alimentarse con los frutos espontáneos de la tierra. Al no tener con qué subsistir, algunos murieron y muchos otros hubieran muerto de no haberse puesto a trabajar la tierra. Y, a medida que la población se multiplicaba, nuevas franjas de bosque tuvieron que ser taladas, desbrozadas y cultivadas. En cada momento de su historia, la humanidad sólo trabaja bajo la amenaza de muerte: toda población, en caso de no encontrar recursos nuevos, está destinada a extinguirse; y, a la inversa, a medida que los hombres se multiplican emprenden trabajos más numerosos, más lejanos, más difíciles, menos fecundos de inmediato. El desplome de la muerte se hizo más temible en la proporción en que las subsistencias necesarias se hicieron más inaccesibles; a la inversa, el trabajo debió aumentar en intensidad y utilizar todos los medios para ser más prolífico. Así, pues, lo que hace posible, y necesaria, la economía es una situación perpetua y fundamental de escasez: frente a una naturaleza que, en sí misma, es inerte y, a no ser por una parte minúscula, estéril, el hombre arriesga su vida” (FOUCAULT, M. 1976:251)⁶⁵.

El trabajo, como condición humana, que desafía la finitud del hombre, se convertirá en el motor de la producción de relaciones sociales y económicas

⁶³ CASTELLS, Manuel. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I*. México: Siglo XXI Editores, 7ª ed., p. 229.

⁶⁴ BAUMAN, Zygmunt. (2003). *Modernidad Líquida*. Buenos Aires: Fondo de Cultura Económica, p. 14.

⁶⁵ FOUCAULT, Michel. (1966). *Las palabras y las cosas*. Madrid: Siglo XXI Editores., p. 251.

complejas en la medida en que la relación entre el medio/naturaleza y el aumento de la población requiere de formas de organización y de gubernamentalidad. Los medios que utilizará el trabajo para ser más prolífico, están en relación directa con el conocimiento. De ahí la división clásica, desde Smith y Marx, de las modalidades del trabajo: el trabajo corporal y el trabajo intelectual, uno dirigido hacia la producción de bienes y mercancías, otro, dirigido a la producción de conocimiento. Según los modos de producción prevaleciente en determinada época, cobrará mayor valor uno u otro tipo de trabajo. Si bien en el trabajo intelectual el compromiso mayor es la producción de conocimiento, en el trabajo corporal también están presentes formas de conocimiento, al menos relacionados con ciertas formas de conciencia. Ya Marx nos lo advertía cuando compara el trabajo material de la abeja, con el trabajo del hombre:

“Pero, hay algo en que el peor maestro de obras aventaja, desde luego, a la mejor abeja, y es el hecho de que, antes de ejecutar la construcción, la proyecta en su cerebro. Al final del proceso de trabajo, brota un resultado que antes de comenzar el proceso existía ya en la mente del obrero; es decir, un resultado que tenía ya existencia ideal. El obrero no se limita a hacer cambiar de forma la materia que le brinda la naturaleza, sino que, al mismo tiempo, realiza en ella su fin, fin que él sabe que rige como una ley las modalidades de su actuación y al que tiene necesariamente que supeditar su voluntad. Y esta supeditación no constituye un acto aislado. Mientras permanezca trabajando, además de esforzar los órganos que trabajan, el obrero ha de aportar esa voluntad consciente del fin a que llamamos atención, atención que deberá ser tanto más

reconcentrada cuanto menos atractivo sea el trabajo, por su carácter o por su ejecución, para quien lo realiza, es decir, cuanto menos disfrute de él el obrero como de un juego de sus fuerzas físicas y espirituales” (MARX, K. 2002)⁶⁶.

Los modos de producción de un tipo de sociedad han estado vinculados con las formas de conocimiento que en esa sociedad imperan. Así, en las sociedades pre-industriales dominaron las formas de conocimiento en el que se privilegiaba la relación con la naturaleza. Sus productos estaban relacionados con la extracción de las materias provenientes de la naturaleza y, para ello, se requerían de saberes de extracción de estos productos: saber sobre la minería, saber sobre los cultivos agrícolas y los cultivos pecuarios, saber sobre la pesca. Pero también, saber sobre la manera de hacer de ellos bienes mercantiles, que adquirieran un valor a ser intercambiado entre diferentes pueblos y culturas. Con la sociedad industrial, las formas de conocimiento variaron. Prevalen los tipos de saberes que permitirán producir saber más, por ello, las teorías de la disciplina, de la medida del tiempo y el espacio que confluyen en una mayor productividad será importante, frente al productor mismo, es decir, frente al obrero. Pero más allá, los medios para producir las mercancías requerirán de tipos de saber afincados en los nuevos descubrimientos científicos. El matrimonio entre ciencia y tecnología iniciará su nueva hegemonía, dirigida hacia una finalidad fundamental, que tiene que ver con las nuevas formas de conocimiento que emergen en la modernidad: el progreso estará íntimamente ligado a la conjunción entre conocimiento-ciencia, tecnología-formas de aplicación del conocimiento y trabajo-como constitución de una forma útil de estar en el mundo del ser humano.

⁶⁶ MARX, Karl. (2002). México: Siglo XXI Editores. *El Capital*.

De esta estrecha relación entre ciencia-tecnología-trabajo aparecen algunos cambios que irrumpen como rupturas con la época anterior. Generalmente se han reconocido tres revoluciones en la época moderna. La primera revolución industrial, a finales del siglo XVIII, está ligada a la aparición de *“la máquina de vapor de Watt, la máquina de tejer de Hargreaves y la metalurgia (que) dan pie a los inicios de la industrialización”*. La segunda revolución industrial, marcada por la emergencia de la *“electricidad, el teléfono y el motor de explosión los que transforman el mundo”*. La tercera, *“nuestra”* revolución industrial, cuyo acontecimiento está en el surgimiento de tres artefactos que dominarán las formas de relación humana con el trabajo y la producción: la aparición de Apartanet para el Departamento de Defensa norteamericano en 1971; de Intel que pone a punto el primer microprocesador en 1976 y la aparición de la computadora que servirá de modelo para los computadores de oficina y luego para los personales (COHEN, D. 2007:25)⁶⁷.

La tercera revolución industrial o tecnológica establecerá las condiciones posibles de existencia de una nueva sociedad, que hoy denominamos la sociedad del conocimiento. Esas condiciones de existencia marcan rupturas con las formas anteriores, aunque se reconoce que no porque se ingrese a una nueva sociedad las otras desaparecen. Por el contrario, el mundo tal y como hoy se presenta, muestra claramente la coexistencia de diversos tipos de sociedad, en las que la relación ciencia-tecnología-trabajo marca sus formas de vida. Sin embargo, la diversidad en los tipos de sociedad y en sus formas de conocimiento ha sido descrita, de manera negativa, como brechas que se presentan como límites frente al “progreso” hacia el nuevo tipo de sociedad y, en sentido positivo, como desafíos para lograr construir este tipo de sociedades (UNESCO, 2007:22)⁶⁸.

⁶⁷ COHEN, Daniel. (2007). *Tres lecciones sobre la sociedad postindustrial*. Buenos Aires: Katz Editores, p. 25,

⁶⁸ UNESCO. (2005). *Hacia la sociedad del Conocimiento*. Paris: Unesco, p. 22.

El documento de la UNESCO, *Hacia las sociedades del conocimiento*, marca la dirección de la relación clásica entre conocimiento-tecnología-trabajo e introduce el papel esencial de la educación en este proceso de cambio:

“El mundo actual —marcado por la explosión demográfica, los imperativos del desarrollo económico y de la lucha contra el hambre, la Revolución científica y técnica, la multiplicación de los conocimientos, la promoción de las masas, las consecuencias y expresiones nuevas de la idea democrática, la extensión y proliferación de los medios de información y de comunicación—, este mundo que plantea y planteará tantas exigencias nuevas a la educación” (UNESCO, 1972:95)⁶⁹.

Y, ¿cuáles son los signos que han posibilitado la emergencia de este nuevo tipo de sociedad? Para responder a esta pregunta debemos remitirnos a las descripciones realizadas por sociólogos y filósofos de la actualidad quienes establecen las características que hoy tensionan la realidad de la condición humana.

En primer lugar, la metáfora de la fluidez, será utilizada para describir la consistencia de la etapa actual de la era moderna. Propuesta por el sociólogo polaco, quien opta por denominar nuestro tiempo como Modernidad Líquida, para definirla de la primera modernidad, cuya consistencia tendría, por el contrario la cualidad de solidez. Nuestra modernidad es líquida, según Bauman, pues la característica principal, que comparte con los fluidos, es el cambio continuo de forma, de posición y, por tanto, con una movilidad en forma de flujo.

⁶⁹ UNESCO. (1972). *Informe Faure. Aprender a aprender*. Paris: Unesco, p. 95.

“Los fluidos, por decirlo así, no se fijan al espacio ni se atan al tiempo... no conservan una forma durante mucho tiempo y están constantemente dispuestos (y proclives) a cambiarla; por consiguiente, para ellos lo que cuenta es el flujo del tiempo más que el espacio que puedan ocupar: ese espacio que, después de todo, sólo llenan por “un momento” (BAUMAN, Z. 2003:7-8)⁷⁰.

Esta metáfora también es propuesta por el sociólogo catalán, Manuel Castells, quien considera que la forma de la modernidad actual, transforma también los conceptos de tiempo y espacio de las formas sociales anteriores. Para él, *“Los flujos no son sólo un elemento de la organización social: son la expresión de los procesos que dominan nuestra vida económica, política y simbólica”*. Los flujos organizan las prácticas sociales en el tiempo. *“Por flujo entiendo las secuencias de intercambio e interacción determinadas, repetitivas y programables entre las posiciones físicamente inconexas que mantienen los actores sociales en las estructuras económicas, políticas y simbólicas de la sociedad”* (CASTELLS, M. 2006:445)⁷¹. De igual forma, Hardt y Negri, consideran el flujo como la principal característica de lo que ellos denominan Imperio, un lugar en un no lugar:

“El imperio se caracteriza por una fluidez de la forma: un flujo y reflujo de formación y deformación, de generación y degeneración...vemos la corrupción no como algo accidental, sino como algo necesario... el imperio

⁷⁰ BAUMAN, Zygmunt. (2003). *Modernidad Líquida*. Buenos Aires: Fondo de Cultura Económica, pp. 7-8.

⁷¹ CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I*. México: Siglo XXI Editores, 7ª ed. p. 445.

requiere que todas las relaciones sean accidentales”

(HARDT. M, y NEGRI. A. 2002:182)⁷².

Si la forma cambia constantemente, gracias a su característica de fluidez, la geometría se hace variable. Igualmente, el espacio y el tiempo, como conceptos centrales al pensamiento occidental, cambian en sus relaciones de interacción, de hegemonía del uno sobre el otro, así como también en su relación con el movimiento. El tiempo y el espacio como estructura de una realidad medible, cuantificable, fue la conquista de la modernidad y la piedra angular de la era industrial. Como lo ilustra Foucault, las disciplinas hicieron posible la inscripción del tiempo y el espacio de producción en el cuerpo del hombre: *“Las disciplinas que analizan el espacio, que descomponen y recomponen las actividades, deben ser también comprendidas como aparatos para sumar y capitalizar el tiempo”* (FOUCAULT, M. 1976:161)⁷³. El tiempo de la modernidad, puede ser dividido en segmentos sucesivos o paralelos, puede ser organizado de manera analítica, tiene un fin. *“Los procedimientos disciplinarios hacen aparecer un tiempo lineal cuyos momentos se integran unos a otros, y que se orienta hacia un punto terminal y estable”*. En suma, un *“tiempo evolutivo”* (HARDT. M, y NEGRI. A. 2002:164)⁷⁴. Con relación al espacio, éste se constituye en “un lugar heterogéneo y cerrado sobre sí mismo” en el que se distribuyen los individuos a través de las técnicas de clausura, localización, emplazamientos funcionales, intercambiabilidad – transformación de las combinaciones, en general, organiza el espacio de manera serial.

⁷² HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, p. 182.

⁷³ HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, p. 161.

⁷⁴ HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, p. 164.

“Al organizar las “celdas”, los “lugares” y los “rangos”, fabrican las disciplinas espacios complejos: arquitectónicos, funcionales y jerárquicos a la vez. Son unos espacios que establecen la fijación y permiten la circulación; recortan segmentos individuales e instauran relaciones operatorias; marcan lugares e indican valores; garantizan la obediencia de los individuos pero también una mejor economía del tiempo y de los gestos” (HARDT. M, y NEGRI. A. 2002:151-152)⁷⁵.

El tiempo y espacio son elementos fundamentales de la praxis humana. En ellos se inscribe y, a la vez, ellos la describen. La modernidad al entender el tiempo como una sucesión lineal, lo concibió como un ascenso o progreso hacia la perfección. La sociedad perfecta, que alberga individuos felices por la satisfacción de una existencia plena, está concebida por su eficacia en los procesos, por la sistematicidad de ellos, por la predicción que de ellos puede realizarse. La eficacia, a su vez, conlleva hacia la concepción de un tiempo más rápido y efectivo. A la economía del movimiento en el tiempo y el espacio. La conjunción ciencia-tecnología, permitieron pensar el tiempo y el espacio bajo la mirada de la “racionalidad instrumental”, como lo expresó Max Weber. Como lo señala Bauman,

“La “conquista del espacio” llegó a significar máquinas más rápidas. Los movimientos acelerados significaban espacios más grandes, y acelerar los movimientos era la única manera de agrandar el espacio. En este caso, la “expansión espacial” era el nombre del juego, y el

⁷⁵ HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada., pp. 151-152.

espacio era la apuesta, el espacio era el valor el tiempo la herramienta” (BAUMAN, Z. 2003:121)⁷⁶.

Pero esta relación tiempo/espacio hoy ha cambiado. El tiempo ha ganado en valor y se impone al espacio. La relación entre uno y otro está marcada por la velocidad y en ella, la creación de un espacio como un “*no lugar*” en tanto no alcanza a perdurar en el tiempo. Constatamos, hoy, que la percepción del espacio y el tiempo ha variado considerablemente. Paul Virilio, el filósofo de la velocidad, nos dice que hoy predomina una tiranía del tiempo real, de la inmediatez, de la ubicuidad, de la instantaneidad. El artificio y la virtualidad imponen el espacio y el tiempo. En cuanto al espacio, encontramos la imperiosa necesidad de generar artificialmente un espacio común en un mundo cada vez más amplio y más vacío en virtud de la incomunicación personal de fondo de los individuos que lo habitan. Ese espacio común se convierte en comunidad, comunidad que anula al sujeto y al yo al imponer como ideal de sí las tendencias de la moda. El sujeto se reconoce en el lugar del poseer y tener todo aquello que se le impone: bienes de consumo, identidades foráneas, conocimientos útiles para la comunidad, más que para sí mismo. En cuanto al tiempo, la soberanía del presente y la inmediatez se convierten en el principal signo. Esta soberanía explicaría la facilidad con que se cambia de identidad, de deseos, de proyectos... la duración depende del instante, pero del instante que impone otro, la comunidad, la moda.

El espacio de la sociedad actual es definido por Hardt y Negri como un lugar que es un no lugar, por su característica de virtualidad:

“La sociedad del espectáculo... es un lugar virtual o, más precisamente, un no lugar... de modo tal que es

⁷⁶ BAUMAN, *Op. Cit.* BAUMAN, Zygmunt. (2003). *Modernidad Líquida*. Buenos Aires: Fondo de Cultura, p. 121.

imposible distinguir lo interior de lo exterior, lo natural de lo social lo privado de lo público. La noción liberal de lo público, el espacio exterior donde actuamos en presencia de otros, ha sido universalizada (porque ahora estamos siempre bajo la mirada de otros, monitoreados por cámaras de seguridad) y a la vez sublimada – o desrealizada- en los espacios virtuales del espectáculo. El fin de lo exterior es el fin de la política liberal” (HARDT. M, y NEGRI. A. 2002:171)⁷⁷.

Castells, por su lado, propone considerar el espacio de la sociedad actual bajo una nueva óptica, diferente a la instaurada por la modernidad. La lógica del espacio de los flujos. El espacio como flujo se diferencia del espacio como lugar en tanto que no aparece como forma sino como proceso. Y, al ser proceso, el espacio estructura el tiempo. En este sentido, Castells se separará de *“las teorías sociales clásicas, que asumen el dominio del tiempo sobre el espacio”*. Su hipótesis propone considerar que *“el espacio organiza al tiempo en la sociedad red”* (CASTELLS, M. 2006:409-410)⁷⁸. Si Hardt y Negri, consideran el espacio como un no lugar, Castells considera el tiempo como atemporal:

“El tiempo atemporal pertenece al espacio de los flujos, mientras que la disciplina temporal, el tiempo biológico y la secuenciación determinada por la sociedad caracterizan a los lugares de todo el mundo, estructurando y desestructurando materialmente

⁷⁷ HARDT Michael. y NEGRI. Antonio. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada, p. 171.

⁷⁸ CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I*. México: Siglo XXI Editores, 7ª ed., pp. 409-410.

nuestras sociedades segmentadas” (CASTELLS, M. 2006:500)⁷⁹.

El tiempo atemporal y el espacio como no lugar, son las características fundamentales de la sociedad actual, en donde lo virtual impera, en el sentido del tiempo instantáneo, la forma constantemente variable por su fluidez, y los espacios que no son forma sino flujos. Estas características de la sociedad actual establecerán las condiciones de posibilidad de la emergencia de dos conceptos que hoy invaden el espacio de la experiencia humana: la globalización y la flexibilidad.

Si el espacio/tiempo de la sociedad moderna permitió la emergencia de la era industrial en el que la experiencia humana podía ser medida, calculada, programada, replicada y cristalizada en una identidad (personal y social); el espacio/tiempo de la sociedad actual, caracterizada como sociedad red, sociedad de flujos, sociedad líquida o sociedad informacional, instituye una experiencia humana que no se dirige hacia una identidad totalitaria sino a una multiplicidad fragmentada. El análisis del trabajo, como forma de organización del tiempo/espacio de la experiencia humana moderna, permitirá también, en la sociedad actual, considerar la naturaleza del cambio. En la era de las disciplinas modernas, el trabajo fue fundamental para estructurar la forma de sociedad que se requería; en la actual era de la información también lo será aunque sus características han variado. Para una y otra época, la relación trabajo/educación es fundamental. Para las disciplinas, la pedagogización del espacio social, se constituyó en la herramienta para dar forma a los individuos que la sociedad necesitaba. Hoy, la educación se constituye en elemento fundamental para preparar al individuo a enfrentarse a una sociedad en constante cambio.

⁷⁹ CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I*. México: Siglo XXI Editores, 7ª ed., p. 500.

En el espacio/tiempo disciplinario, el programa, la segmentación del tiempo con miras a un fin, la preparación para un oficio o una profesión que confieren al individuo una identidad social, serán los que dominarán es espacio formativo:

“Es este tiempo disciplinario el que se impone poco a poco a la práctica pedagógica, especializando el tiempo de formación y separándolo del tiempo adulto, del tiempo del oficio adquirido; disponiendo diferentes estadios separados los unos de los otros por pruebas graduales; determinando programas que deben desarrollarse cada uno durante una fase determinada, y que implican ejercicios de dificultad creciente; calificando a los individuos según la manera han recorrido estas series” (FOUCAULT, M. 1976:163)⁸⁰.

En el espacio/tiempo de la sociedad actual, la variación, la flexibilidad en el tiempo y en el espacio, la preparación para la variabilidad de las identidades que deben ser asumidas según lo imponga el momento y las circunstancias – siempre variables- serán los desafíos del acto formativo. Si el trabajo constituía una manera de estar en el mundo del individuo, acceder a un lugar o puesto de trabajo era la aspiración de la educación para la vida y, por tanto, adquirir una identidad estable, una pertenencia a un oficio, a unos saberes, a una profesión; en la actualidad el cambio en la forma del trabajo determina también un cambio en la manera de concebir la formación del individuo para el trabajo. Si en la sociedad industrial el saber y el conocimiento utilizados en por la fuerza laboral estaban principalmente encaminados a la producción de bienes de consumo; en la sociedad post-industrial es la producción de

⁸⁰ FOUCAULT, Michel. (1966). *Las palabras y las cosas*. Madrid: Siglo XXI Editores, p. 163.

conocimiento y de información la que prevalece sobre la producción de bienes.

1.5.1. Configuración de la cultura global y construcción de la identidad

JAVIER BUSTAMANTE, en su obra FILOSOFÍA DE LA INFORMACIÓN Y DEL CONOCIMIENTO plantea claramente las consecuencias e impacto del internet en la sociedad, cuando cita: *“A pesar de los riesgos de una eficacia totalizadora y la inercia mental que podría desembocar en una progresiva deshumanización, pocos dudan ya del impacto que la tecnología informática a través de Internet está comenzando a tener en la configuración de la cultura global del siglo XXI.”*

El impacto de los avances tecnológicos, la cultura global y en palabras del autor, *Internet pone en jaque el concepto de territorialidad, pues las comunidades que nacen en su seno, las llamadas redes virtuales, no tienen como elemento de unión un espacio físico, una etnia o un idioma compartidos.* BUSTAMANTE DONAS, J. (2009:99)⁸¹ Con la aseveración anterior coincidimos conceptualmente con el autor en cita, cuando establecemos que los aspectos metodológicos de la presente investigación van encaminados a solucionar los baches de competencia y territorialidad que en el ámbito jurídico han generado las relaciones sociales, personales y comerciales a través del mundo virtual. Así mismo BUSTAMANTE DONAS⁸² *Cuestiona los modelos económicos vigentes, pues en ella los bienes digitales tienen valor no en función de su escasez —según los dictados de la ley de la oferta y la*

⁸¹ BUSTAMANTE DONAS, J. Universidad Complutense de Madrid. (2009:99) En: SUÑÉ LLINÁS, E. (2009) Filosofía jurídica y política de la nueva ilustración. Estudios en homenaje a la Escuela Libre de Derecho en su primer centenario. México D.F.: Porrúa.

⁸² BUSTAMANTE DONAS, J. Universidad Complutense de Madrid. (2009:99) En: SUÑÉ LLINÁS, E. (2009) Filosofía jurídica y política de la nueva ilustración. Estudios en homenaje a la Escuela Libre de Derecho en su primer centenario. México D.F.: Porrúa.

demanda—, sino de su omnipresencia. Las comunidades de intercambio y su pugna en pro del conocimiento libre ponen en tela de juicio los conceptos tradicionales de propiedad intelectual, de control de la información, de copia y reproducción. A partir de ellas se ha extendido una metáfora de solidaridad, libre colaboración y sinergia frente a competencia, que transforman el concepto de negocio, cuestionando la separación tradicional de los papeles de productor y consumidor. Todo lo que es digital puede existir en Internet, y la digitalización homogeneiza todo tipo de datos: música, películas, textos, etc. Todo ello está ya creando un nuevo paradigma ético propugnado desde el movimiento de Software Libre, donde la sinergia se opone a la competencia, y donde la escasez de un bien no lo hace más valioso, sino al contrario. (BUSTAMANTE DONAS, J. 2009:99)

1.6. Definición de la información o el dato

El significado filosófico y científico de la palabra información ha sido objeto de múltiples debates. Así pues, desde un punto de vista etimológico, la palabra información viene de la raíz latina *forma* y, como tal, la información es, simplemente, un conjunto de datos transmitidos desde una "fuente" emisora hasta una "fuente" receptora. De este modo, la transmisión de información no implica necesariamente la transmisión de conocimientos, de tal manera que incluso las máquinas son capaces de informar, pues la información únicamente es la una unión coherente de datos que, sin tener en cuenta la interpretación de estos, constituyen formalmente la información (MARQUEZ ESCOBAR, P. C., 2002:20)⁸³. Para otros, con los que nos identificamos, la información *"parece admitir forzosamente la noción de conciencia y sentido"*

⁸³A favor de este punto se pronuncian Ferrater Mora, José. (2012). *Diccionario de Filosofía. Tomo I*. Madrid: Ariel Filosofía, p. 1839.; Crosson, Frederick y Saire, Kenneth. (1982). *Filosofía y Cibernética*. México: Fondo de la Cultura Económica. También en Corte Constitucional, sentencia T-414 de 1992. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Leyer: Bogotá D.C. p. 20.

(MARQUEZ ESCOBAR, P. C., 2002:20)⁸⁴, de modo que, sólo puede haber procesos de información entre entes que tengan conciencia con la cual le puedan asignar a tales datos un sentido, en principio hombres, lo cual no nos puede llevar a descartar la posibilidad de la conciencia de las "máquinas" (MARQUEZ ESCOBAR, P. C., 2002:20)⁸⁵. Así pues, algo sólo se convierte en información cuando algún agente cognitivo le asigna una significación, es decir, lo interpreta como signo" (MARQUEZ ESCOBAR, P. C., 2002:21)⁸⁶. La información, vista desde el sujeto, solamente puede ser percibida cuando tal sujeto puede asignarle sentido.

Desde un punto de vista formal y objetivo, la información es datos, debido a que la estructura de los procesos informáticos se fundamenta en aquellas partículas, lo que permite que sea transmitida por un sujeto no consciente pero que necesariamente sea enviada y recibida por entidades que consideren que dichos datos contienen una significación cognitiva. Así lo dijo la Corte Constitucional Colombiana, en la sentencia T-414 del año 1992, al acoger en la sentencia la consulta hecha al experto ERNESTO LLERAS quien observa, según dice la Corte, que:

"En la teoría de la información el dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que

⁸⁴Ruyer, Raymond. *La cibernética y el origen de la información*, traducción de Córdoba y Magro, Mercedes, México, Fondo de la Cultura, p. 11. En el mismo sentido, cfr. Dretske, Fred, *Conocimiento e información*, Madrid, Salvat, 1987. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer p. 20.

⁸⁵Los sorprendentes avances de la ciencia han llevado a la creación de sistemas autómatas que responden a los datos evaluando los distintos sistemas de información, tal como lo hizo recientemente la computadora Deep Blue de la I.B.M. que siendo "programada" para jugar ajedrez realizó varias jugadas que parecían no responder a los principios lógicos que maneja un computador normal pues engañó al campeón del mundo de ajedrez ejecutando una jugada que a los ojos de los expertos no parecía ser efectiva. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*, Bogota D.C.: Leyer, p. 20.

⁸⁶Dretske, Fred. (1987). *Conocimiento e información*. Madrid: Salvat, p. 1. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*, Bogota D.C.: Leyer, p. 21.

dicho dato adquiera sentido. ...Se puede decir que el sentido, en última instancia, lo producen una o varias mentes humanas, y este sentido es un determinante de la acción social. Los modelos se plasman en forma de textos y mensajes que consisten en una serie de signos, algunos de los cuales le llamaremos datos, organizados de acuerdo con sistemas de reglas o gramática. A través de los signos y mensajes los eventos adquieren realidad social. La realidad expresada a través de mensajes... es la determinante de la acción social. El dato se constituye entonces en el elemento básico de información sobre eventos o cosas" (MARQUEZ ESCOBAR, P. C., 2002:21)⁸⁷.

La teoría de la información que fundamenta este trabajo se sustenta en que todo tipo de información está compuesta de datos y, en que es el receptor consciente quien interpreta tales datos para que, al encasillarlos dentro de su sistema mental, se conviertan en elementos con significado. Así, los datos se convierten en un elemento necesario en toda estructura de transmisión de información.

La palabra dato viene del verbo latino *daré*, término utilizado en la edad media como *datum*, concepto que aludía a una simple fecha. La evolución terminológica lo llevó a ser considerado una parte de la estructura de la información por su uso contable informativo para los comerciantes burgueses. Teóricamente, los datos son formados por caracteres, y los caracteres son de tipo numérico y alfanumérico, siendo estos últimos la mínima unidad del

⁸⁷Corte Constitucional, sentencia T-414 de 1992, Magistrado Ponente Dr. Ciro Angarita Barón, Santafé de Bogotá, 16 de junio de 1992. Las cursivas son nuestras. Con éste tipo de decisiones la Corte, en sus primeros días de vida, parece fundamentar sus decisiones sobre la información en cierto modelo teórico de la comunicación, pero como veremos más adelante, este organismo colegiado pierde su norte en otras sentencias donde hace caso omiso a este pronunciamiento y sin pronunciar una nueva teoría de la información coherente dicta sentencia sobre el tema sin tener en cuenta las Implicaciones filosófico-jurídicas. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). El delito Informático. Bogota D.C.: Leyer p. 21.

proceso de comunicación. Dentro de la informática, es decir, ciencia que estudia la información y los medios de transmisión de información para el procesamiento y almacenamiento, la acumulación de varios datos se llama "datos agregados"; a la unión de estos, "registro"; a la colección de varios registros se le llama "*archivo*" y, la unión de varios "*archivos*", con un único propósito, se llama base de datos.⁸⁸

Además, para completar un bosquejo de una teoría de la información, hay que distinguir entre información y comunicación. El proceso de comunicación comprende al de la información, pues es con ésta que se da la comunicación. El mensaje de datos que envía el emisor le llega al receptor a través del canal o medio de transmisión. Estos sólo se *transforman* en información en el momento en que el receptor capta los datos transmitidos. De esta manera, pues, el proceso de comunicación contiene el proceso de información, pero se diferencia de aquél en que hay una transmisión de respuesta a la información enviada, de modo que se da un proceso de alimentación externa de los datos enviados.

De todo lo anterior, encontramos que en todo proceso informático es necesario el cotejo de datos. Estos datos están dados en un Código, que en los computadores actuales es binario, es decir, por medio de las cifras 1 y 0 - con los nuevos avances en poco tiempo serán trinarios. De ese modo, el procesamiento de datos se hace en Códigos que el procesador asimila, convierte y procesa en su propio *lenguaje* y, luego, los reconvierte a través de un Código de salida. Precisamente, para la comunicación, el dato se hace esencial pues es la unidad mínima de la información y la información es la unidad fundamental del proceso comunicativo.

⁸⁸Villanueva Lara, Julio. (1981). *Introducción a la Computación*. Washington: O.E.A., p. 73. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer p. 22.

Para concluir, con la aparición de nuevas tecnologías de la información la recolección, almacenamiento, flujo y transmisión de datos se ha ido facilitando, pero, sin lugar a dudas, el avance más importante en tal proceso ha sido la creación de la computadora, pues ésta ha permitido que el almacenamiento y el flujo de información se aceleren y, sobre todo, ha permitido que la colección y recolección de los datos se haga de manera accesible y segura. Además, la unión de las tecnologías de la información con las telecomunicaciones ha permitido que el cotejo de información sea indirecto, es decir, que se pueden consultar los datos desde terminales apartadas de la base de datos de modo que el acceso es cada vez más sencillo (MARQUEZ ESCOBAR, P. C., 2002:22)⁸⁹.

Ya encontramos que dentro de la cibernética, el elemento fundamental es la información y que, dentro de ésta, se halla el dato como elemento básico de la informática que, al final de cuentas, comparte su objeto de estudio con la cibernética (MARQUEZ ESCOBAR, P. C., 2002:20)⁹⁰.

1.7. Desarrollo histórico del concepto de información o dato

Desde fines del siglo XIX hasta mediados del siglo pasado, las tecnologías de la información han mantenido un papel protagónico en el desarrollo de la sociedad. En respuesta a tal fenómeno, se emprendieron múltiples escritos sobre la llamada teoría de *la información* o *teoría de la comunicación*, que tenían como objeto de estudio establecer cuál era la influencia sobre las esferas económica, jurídica y social. Se pensaba que la sociedad capitalista estaba cambiando, que habíamos superado la modernidad y que el papel del

⁸⁹ Cfr. Fitzgerald, Jerry y Eason, Tom. (1986). *Fundamentos de comunicación de datos*, México: Limusa. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 22.

⁹⁰MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 20-22.

hombre en la sociedad daría un vuelco tal, que la concentración de los medios de producción dejaría de ser el elemento de poder por excelencia, para darle su lugar a la información como nuevo elemento propio de quien está en el poder.

Así, se realizaron múltiples investigaciones como la de DANIEL BELL en 1973. (MARQUEZ ESCOBAR, P. C., 2002:17)⁹¹, ZBIGNIEW BREZEZINSKI en 1973 (MARQUEZ ESCOBAR, P. C., 2002:17)⁹², MANUEL GARCÍA PELAYO en 1974 (MARQUEZ ESCOBAR, P. C., 2002:17)⁹³, SIMÓN NORA y ALAIN MINC en 1981 (MARQUEZ ESCOBAR, P. C., 2002:20)⁹⁴ y HERBERT SCHILLER en 1983 (MARQUEZ ESCOBAR, P. C., 2002:20)⁹⁵, que continuaron el desarrollo de los estudios iniciados en la época de la posguerra por un conjunto de matemáticos y científicos norteamericanos, encabezados por CLAUDE E. SHANON y NORBERT WIENER.

SHANON, en su estudio publicado en 1948 y titulado *Mathematical theory of communication* (MARQUEZ ESCOBAR, P. C., 2002:17)⁹⁶, formuló los principios matemáticos que han sustentado desde entonces la teoría de la información. Y WIENER, en el escrito titulado *Cybernetics*, hizo pública la importancia de las comunicaciones en la mayoría de las ciencias, en la sociedad y en el campo

⁹¹Bell, Daniel. (1976), *El advenimiento de la sociedad posindustrial*. Madrid: Alianza. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 17.

⁹²Brezekinski, Zbigniew. (1973). *La era tecnológica*. Buenos Aires: Paidós. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 17.

⁹³García Pelayo, Manuel, *Burocracia y tecnocracia y otros escritos*, Madrid, Alianza, Fondo de la Cultura Económica, 1974. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.17.

⁹⁴Nora, Simón; Minc, Alain, *La informatización de la sociedad*, México, Fondo de la Cultura Económica, 1981. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 17.

⁹⁵Schiller, Herbert, *El poder informático*, Barcelona, Gustavo Gili, 1983. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.17.

⁹⁶Shanon, Claude E., *A mathematical theory of communication*, en *Bell System Técnica! Journal* 27 (1948), citado por Crosson, Frederick y Saire, Kenneth, *Filosofía y Cibernética*, México, Fondo de la Cultura Económica, 1982. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.17.

jurídico (MARQUEZ ESCOBAR, P. C., 2002:17)⁹⁷. Teniendo como base estos estudios, los estudios sociológicos emprendidos a fines de los años setenta y principios de los ochenta llegaron a importantes conclusiones. Se demostró, en el campo económico, cómo el papel del sector servicios, en las economías nacionales, incrementó enormemente su producción con relación a los otros sectores reales de la economía, generando un flujo de capitales del sector industrial al sector servicios, de la misma manera como sucedió en tiempos atrás con la revolución industrial donde el flujo se dio del sector agrícola al sector industrial. Asimismo, la educación comenzó a tomar un papel más relevante dentro de la sociedad. Los esfuerzos estatales por incrementar la alfabetización de principios de siglo se vieron complementados con el fortalecimiento de las instituciones de educación privada, con lo que se afianzaron las profesiones liberales debido a su utilización en procesos industriales.

Con la explosión educativa, la información técnica y teórica proliferó en las universidades y en los numerosos centros de investigaciones que se fundaron a fines del siglo XIX y principios del siglo pasado; también se dio una mayor importancia a nuevas ciencias, como la estadística y la econometría. Así, con el nacimiento de ésta, y con la percepción de que la información que ella proveía era un elemento fundamental para la toma de decisiones económicas, los dueños de los medios de producción comenzaron a acaparar dichos "*bienes informáticos*". De este modo, se desarrollaron métodos para el fácil y rápido cotejo de información: se inventó el teléfono, el telégrafo, la máquina de escribir, etc. El traspaso de información cada vez fue más rápido, a pesar de ser más formal debido a la utilización de códigos y claves virtualmente inmodificables.

⁹⁷Wiener, N. *Cybernetic*,. Cambridge. Mass: M.I.T. Press, 1948, citado por Crosson, Frederick y Saire, Kenneth, *Filosofía y Cibernética*, México, Fondo de la Cultura Económica, 1982. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.17.

Además de aquellos desarrollos de las tecnologías de la información, en los primeros años del siglo XX se creó una de las tecnologías de la información que cambiaría radicalmente el proceso de almacenamiento, catalogación y recuperación de información: el *computador electrónico*. Antes existían computadores mecánicos que, mediante procesos estructurados con piñones y palancas, permitían realizar cálculos como sumas, restas, multiplicaciones, etc. Pero fue sólo cuando se ingenió el sistema electrónico, que se llegó a pensar en el mejor aprovechamiento del computador como sistema de procesamiento de información. Con la invención del transistor, la velocidad de procesamiento mejoró y, con él, el ascenso en la velocidad y la capacidad de almacenamiento de información. Se crearon las bases de datos y el cotejo de información fue cada vez más fácil, más directo y más rápido. Incluso los más osados consideraron crear bases de datos y sistemas que resolvieran directamente cuestiones jurídicas (MARQUEZ ESCOBAR, P. C., 2002:18)⁹⁸. Además, se generaron institutos para el desarrollo de un pensamiento filosófico como respuesta al papel de la computadora en la sociedad, tal como sucedió en la Universidad de Notre Dame (MARQUEZ ESCOBAR, P. C., 2002:18)⁹⁹.

Estos avances tuvieron muchos detractores quienes fundamentaron sus críticas en el manejo que se le estaba dando a las nuevas tecnologías de la información. Vieron en las computadoras y sus gigantescas bases de datos una amenaza a su intimidad, a la privacidad, e incluso una amenaza contra la democracia misma, pues con el manejo incontrolado de tales tecnologías se permitía el fortalecimiento de la vigilancia estatal y, peor aún, dieron cuenta

⁹⁸Para una referencia amplia sobre el tema consultar: Frosini, Vittorio. (1978). *Cibernética, derecho y sociedad*. Madrid: Tecnos. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.18.

⁹⁹Instituto filosófico para la inteligencia artificial, University of Notre Dame, Pennsylvania, Creado en 1965. Citado en MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.18.

de la transformación de las instituciones del Estado al observar que su papel frente a la sociedad civil se estaba comercializando, al utilizar la *vigilancia electrónica de los ciudadanos* como medio de control para lograr el pago de tributos. De la misma forma, el papel del comercio y de los comerciantes comenzó a estatizarse, en la medida en que ellos tomaron para sí la función conductora de la sociedad civil que ostentaba el Estado moderno para luego ejercer la vigilancia con un matiz disciplinador (MARQUEZ ESCOBAR, P. C., 2002:23)¹⁰⁰.

En busca de mejorar el desempeño de tales funciones, la informática, entendida como ciencia que estudia la información y los medios de transmisión de información, surgió como el centro de atención sobre el cual giraron cada uno de los desarrollos tecnológicos del siglo pasado. Así, la industria de las telecomunicaciones, como principal medio de transmisión de información, ostenta el mayor índice de crecimiento en la última década del siglo pasado y la razón fundamental de ello es que el hombre actual vive y se desarrolla en un medio donde los datos, la información y la comunicación son parte fundamental de la vida diaria.

Como consecuencia de lo anterior, la información se ha desempeñado últimamente en la vida del hombre como el "*bien*" que más estiman las organizaciones capitalistas por su potencialidad para generar grandes

¹⁰⁰Este punto ha sido objeto de múltiples debates en la doctrina nacional e internacional. La proliferación de bases de datos sobre personas ha generado conceptos como la "dataimagen", sustentada como el "yo" del sujeto en una base de datos; "Yo" distinto a "yo" real. En países más desarrollados existen miles de bases de datos en las que se manejan una infinidad de datos personales disfrazados en números como el de la Seguridad Social en Estados Unidos, donde con el solo acceso a la base se puede tener un perfil psicológico, sociológico, económico y jurídico de cualquier persona. Para un estudio más detallado sobre el tema ver: Lyon, David. (1994). *El ojo electrónico: el auge de la sociedad de vigilancia*. Santafé de Bogotá: Alianza; también: Negroponte, Emanuel. (1995). *Digital Belng*. Buenos Aires: Atlántida. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.19.

utilidades. Y tal como pasó siglos atrás con la propiedad del suelo¹⁰¹, la protección de la información desde lo jurídico se hizo a sí misma necesaria, por su capacidad para potenciar el desarrollo económico (MARQUEZ ESCOBAR, P. C., 2002:17-19)¹⁰².

En las últimas décadas del siglo XX, la información ha tomado un valor económico en el contexto jurídico y social. Las implicaciones económicas y sociales de la información han generado conceptos teóricos que se contraponen a las categorías jurídicas vigentes y, a pesar de que el sistema jurídico colombiano pareciera adoptar fácilmente en su estructura a la información en su doble matiz, como derecho fundamental y como bien sujeto al derecho de propiedad, hay ciertas instituciones jurídicas que se hacen inconmensurables. Por ejemplo, la propiedad informática enfrentada a ciertas instituciones jurídicas como el *habeas data*, el derecho al buen nombre y el derecho a la honra parecen estar inmersos dentro de las categorizaciones de lo público y lo privado que fundamentan nuestro sistema y que, como tales, tuvieron mucha fuerza en la modernidad, pero que con la evolución jurídica contemporánea su acoplamiento ha sido cada vez más conflictivo, pues estas concepciones han venido vahando debido al dinamismo social y al aceleramiento de los procesos de comunicación y socialización.

Por lo anterior, el análisis que haremos sobre la información como derecho político, tendrá en principio dos partes, una referida al primer matiz de la información, es decir, el derecho constitucional de la información en su concepto y su evolución. Asimismo, analizaremos también los conflictos normativos o entre derechos, y la extraña involución de la jurisprudencia constitucional en la materia. Luego, haremos un análisis de la información en su segundo matiz, es decir, como elemento que hace parte de los derechos

¹⁰¹ Carnelutti, Francesco. (2000). *Cómo nace el derecho*. Santafé de Bogotá: Temis. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.19.

¹⁰² MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 17-19.

de propiedad legítimamente reconocidos (MARQUEZ ESCOBAR, P. C., 2002:25)¹⁰³.

1.8. La información como objeto del derecho

1.8.1. La información en la historia Constitucional

En el informe 19c/93, publicado por la UNESCO el 16 de agosto de 1976, se presentó a la comunidad internacional la importancia que en las últimas décadas del siglo XX iba a tener la información. Lo fundamental de tal informe es que culminó, en cierto modo, los esfuerzos sociales emprendidos para lograr el reconocimiento general de los derechos fundamentales de la información. En el informe, la UNESCO sintetizó con las siguientes palabras dichos esfuerzos, así:

"Mientras la comunicación interpersonal fue la única forma de comunicación humana, el derecho de la libertad de opinión era el único derecho de la comunicación. Más adelante con la invención de la imprenta se añadió el derecho a la libertad de expresión. Y más tarde aún, a medida de (sic) que se desarrollaban los medios de comunicación, el derecho a buscar, recibir e impartir información pasó a ser la preocupación fundamental" (UNESCO, 1976:25)¹⁰⁴.

Teóricamente, desde el nacimiento de las teorías sobre la naturaleza y la dignidad humana, la noción de libertad de pensamiento parecía de suyo connatural y esencial al hombre, de manera que por muchos esfuerzos que se hiciesen por limitar esta libertad nunca se podría tener éxito, a menos que

¹⁰³ MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogotá D.C.: Leyer, p.25.

¹⁰⁴ UNESCO. Informe 19c/93 de 16 de agosto de 1976. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogotá D.C.: Leyer, p. 25.

se hiciera de la manera en que se sugirió en la célebre obra de ciencia-ficción un *mundo feliz* (MARQUEZ ESCOBAR, P. C., 2002:26)¹⁰⁵.

En nuestro concepto, la libertad de pensamiento es innegable en los seres humanos, hasta el punto que, aunque las normas pretendan negarle su carácter autónomo, la condición pensante del sujeto hace que las normas que limitan su pensamiento sean inoperantes.

El punto de partida de cualquier estudio sobre la información debe ser el pensamiento, pues como principal valor del humano materializó las convenciones que han hecho posible la información: el lenguaje. Parece claro que la expresión de pensamientos ha hecho del hombre lo que es. La expresión codificada convencional que se dio con la elemental generación de sonidos ha permitido al hombre comunicarse, lo mismo que la codificación y la categorización de tales señales sonoras en términos gráficos que, en cierto modo, se convirtieron en expresiones *racionales* del pensamiento humano. La expresión del hombre se convierte en pilar fundamental del desarrollo, pues cada cultura asienta sus registros históricos a través de actitudes lingüísticas y grafológicas que permiten que todo hombre participe de la historia comunal y que, además, a través del proceso de comunicación pueda desarrollar su condición política, económica y cultural. En este sentido, autores como VERNANT (MARQUEZ ESCOBAR, P. C., 2002:26)¹⁰⁶, consideran que el desarrollo del pensamiento en la *polis* griega se debió a tres causas, destacando como fundamental el desarrollo y expresión del *logos* y su uso en el entorno político de la ciudad (MARQUEZ ESCOBAR, P. C., 2002:26)¹⁰⁷.

¹⁰⁵Huxley, Aldous Leonard, *Un mundo feliz*, México, Porrúa, 1994. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

¹⁰⁶Cfr. Vernant, Jean-Pierre. (1992). *Los orígenes del pensamiento griego*. Barcelona: Paidós, Colección Studio. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

¹⁰⁷Vernant, Jean Pierre, *Ibíd.*, ver introducción. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

También HEGEL (MARQUEZ ESCOBAR, P. C., 2002:26)¹⁰⁸ reconoce la importancia de la expresión, pues consideró que para que una cultura pudiera desarrollar un pensamiento filosófico era necesario que en el contexto social se tuviera la libertad de expresión como la facultad humana que permite el desarrollo del pensamiento (MARQUEZ ESCOBAR, P. C., 2002:26)¹⁰⁹.

Jurídicamente, el desarrollo de la libertad de expresión comienza con el Código de Manu, en el cual se consagró, por primera vez, la libertad de pensamiento en uno de los 2.685 versos que se conservan de la llamada *Manu Smṛiti*, ley de Manu o "*Código de las diez libertades humanas esenciales y controles o virtudes necesarias para la vida buena*" (MARQUEZ ESCOBAR, P. C., 2002:26)¹¹⁰. Posteriormente, aparecieron algunos escritos griegos y romanos sobre la libertad de expresión que cuentan sobre la censura a ciertas opiniones en el mundo antiguo (MARQUEZ ESCOBAR, P. C., 2002:27)¹¹¹, como las mencionadas por PLATÓN en el discurso de Pausanias del Banquete (MARQUEZ ESCOBAR, P. C., 2002:27)¹¹², donde se deslumbra el relativismo cultural y respecto de la pederastia en la Grecia Antigua. Con el desarrollo del pergamino y las técnicas de escritura se generaron ciertas limitaciones a la libertad de expresión, pues tales tecnologías de la información atentaban contra los poderes políticos constituidos. En la Roma Antigua, siguiendo la herencia griega, se respetaron en cierto modo tales libertades sólo a quienes las podían tener, es decir, a aquellos que dentro de la estratificación social romana tenían derechos constituidos y reconocidos por

¹⁰⁸Hegel, W.G.F. (1977). *Lecciones sobre la historia de la filosofía*, Tomo I, México: Fondo de la Cultura Económica, 1977. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

¹⁰⁹Hegel, *Ibíd.*, p. 52 a 56 y 90 a 96. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

¹¹⁰González, Cristóbal. (1992). *De la libertad de expresión a la libertad de información*, Revista Universidad INCCA, abril de 1992, Santafé de Bogotá, p. 24. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 26.

¹¹¹Cfr. Gil, Luis. (1985). *La censura en el mundo antiguo*, México: Alianza. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 27.

¹¹²Platón. (1992). *El banquete*. Madrid: Aguilar. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 27.

su calidad de ciudadanos romanos. Justamente, las libertades eran las que el hecho de ser ciudadano les concedía. Por esta razón, autores como DESANTES, establecen que "la libertad de expresión en el mundo antiguo no fue más que eso, libertad; comoquiera que no encontró obstáculo qué vencer, a diferencia de las otras libertades, no encontró argumentos apologéticos a su favor". (MARQUEZ ESCOBAR, P. C., 2002:27)¹¹³

Distinta opinión tiene GILÍ (MARQUEZ ESCOBAR, P. C., 2002:27)¹¹⁴ quien considera que, en el mundo antiguo, tal libertad tuvo obstáculos a vencer, tales como la mediación en la transmisión de textos, con la cual se realizaban "*expurgos*" en ellos y se restringía la circulación de aquellos que, según las luchas ideológicas y religiosas de los distintos períodos, discrepaban con los valores morales vigentes. Aun así, nunca hubo una positivización del concepto libertad de expresión en el mundo antiguo.

Con la expansión de la cultura latina y la imposición de las doctrinas judeo cristianas, el medioevo occidental se convirtió en un mundo de censura y estancamiento tecnológico. La secularización del pensamiento occidental llevó a que sólo pocos textos pudiesen ser copiados y sólo pocos tuvieran acceso a ellos. En esta etapa de la cultura occidental, la libertad de expresión se redujo a una élite mínima y, por este mismo motivo, el desarrollo de las tecnologías de la información se estancó, pues no había quién las solicitase, ya que la poca demanda de éstas la satisfacían los primitivos medios de multicopiado a través del dictado sobre pergamino. En contraste, la reacción del mundo oriental fue distinta. El poder político dominante en el medioevo llevó al desarrollo de la cultura china, donde se inventaron elementos industriales, tales como el alto horno en el año 200 d.c., aún utilizado en las

¹¹³ *Ibíd.*, p. 47. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 27.

¹¹⁴ Gilí, p. 21,111 y ss. Citado en: MÁRQUEZ ESCOBAR, P.C., *Op. Cit.*, MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 27.

acerías del mundo, al igual que las embarcaciones oceánicas, que les permitían emprender largos viajes marítimos (MARQUEZ ESCOBAR, P. C., 2002:28)¹¹⁵. Aparte de estos hallazgos, en la cultura China de la información, se presentaron grandes descubrimientos. Fueron los inventores del papel y de la imprenta, actitud que los tuvo, en opinión de JONES (MARQUEZ ESCOBAR, P. C., 2002:28)¹¹⁶, "a un ápice de la industrialización en el siglo XIV" (MARQUEZ ESCOBAR, P. C., 2002:28)¹¹⁷, pues como lo establece DESANTES, con la imprenta el desarrollo de la libertad de expresión hubo un desarrollo de la industria y el comercio (MARQUEZ ESCOBAR, P. C., 2002:28)¹¹⁸. Estos ejemplos son plena prueba de cómo el impulso del poder gobernante en el Estado hace que ciertos tópicos jurídicos y sociales se desarrollen más que otros, pues, los grupos sociales con poder político exigen al grupo político gobernante la garantía de que las limitaciones existentes se mantendrán entre tanto les convenga. Por dichas actitudes políticas, se dan las primeras revoluciones que culminarían con las declaraciones de derechos. Las primeras declaraciones fueron exigidas por los señores feudales al Reino Inglés, quienes reconocieron, entre otras cosas, la libertad de nombrar sus caballeros y la de heredar su feudo. Estas llamadas "libertades privilegio", se constituyeron en textos como la *carta magna* de JUAN I de Inglaterra -Juan sin Tierra-, donde se estableció la primera regulación de las relaciones entre el rey y la nobleza, se garantizaban los derechos feudales, se establecía un sistema judicial, se eliminan la mayoría de los abusos de los derechos feudales, se protegió el comercio al garantizar las libertades de Londres y de otras ciudades, municipios y puertos de Inglaterra, se garantizó la libertad

¹¹⁵ Castells, Manuel. p. 34. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 27.

¹¹⁶ Jones, Eric L. (1980). *Growth Recurring: Economic Change in World History*, Oxford: Clarendon Press. Citado en: Mokyr, Joel. (1990). *The Travel of the Riches*, Technological Creativity and Economic Progress, Oxford: Oxford University Press. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 28.

¹¹⁷ Jones, Eric L, p. 160. Citado en: MÁRQUEZ ESCOBAR, P.C., *Op. Cit.*, p. 28.

¹¹⁸ Cfr. Desantes, José María. (1977). *Fundamentos del derecho de la información*. Madrid: Editorial Confederación Española, p. 46. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 28.

comercial para los extranjeros y se estableció un sistema de pesos y medidas (MARQUEZ ESCOBAR, P. C., 2002:28)¹¹⁹. Dichas disposiciones fueron confirmadas en "*confirmatio cartorum*" de 1279.

Con el "*Bill of Rigths*" de 1629 y el "*Habeas Corpus Rigth*" de 1679 se ampliaron y confirmaron los derechos de la clase comerciante, clase que emergería de lo profundo del escalafón social para convertirse, hoy por hoy, en la "clase" dominante. Luego de tales declaraciones se le daría vida a la más importante de todas, pues fue la que culminó el proceso de declaraciones de derechos en Inglaterra, la "*declaration of Rigths*" de 1689. Esta declaración estaba inmensamente influida por escritos como el "*Aeropagítica*" de JOHN MILTON, quien ya en 1674 sostenía que las ideas debían circular libremente al igual que las palabras (MARQUEZ ESCOBAR, P. C., 2002:28)¹²⁰. Así, se incluyeron dentro de la "*Declaration of Rigths*" libertades que dieron el inicio de la expansión de las declaraciones constitucionales de derechos y los abundantes escritos sobre teoría política de los ingleses de la Ilustración. Debido a esto, en 1789, la libertad de expresión alcanzó su punto máximo, al ser establecida en la "Declaración de Derechos del Hombre y del Ciudadano" aprobada en el marco de la revolución francesa. Aun así, en Estados Unidos ya se había dado el "*Bill of Rigths*" en 1779, donde se declara la libertad de imprenta, de la misma manera que se hizo años atrás en la Constitución del Estado de Virginia en 1776. La libertad de expresión sólo vino a ser incluida en la primera enmienda en 1791 (MARQUEZ ESCOBAR, P. C., 2002:29)¹²¹.

¹¹⁹Enciclopedia Microsoft® Encarta® 97©, Carta Magna, 1993-1996 Microsoft Corporation. Citado en: MÁRQUEZ ESCOBAR, P.C., *Op. Cit.* MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 28.

¹²⁰González, Cristóbal., *op. cit.*, p. 25. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 28.

¹²¹Desantes, *Op. cit.*, p. 50. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 29.

Estos dos desarrollos en cierto modo fueron, como lo expresa GONZÁLEZ, el logro más grande de la Burguesía contra el poder monárquico (MARQUEZ ESCOBAR, P. C., 2002:29)¹²², pues estos siempre tomaron la censura como medio de represión del poder político de la Burguesía, prohibiendo incluso, aquellos "café" donde se reunía la juventud burguesa educada en Europa en el siglo XVIII.

Posteriormente comenzó el auge del industrialismo y con él el desarrollo del socialismo. Actitud político filosófica que, en vista de las condiciones del pueblo, que debía vender su fuerza de trabajo al mejor postor para poder sobrevivir, encuentra en la socialización de los factores de producción y el control estatal de los recursos económicos, la manera como se equilibrará el ingreso social y se eliminará de tajo la acumulación de capitales tan deseada por el capitalismo. Estas tendencias, genealógicamente comunistas, pretendían justicia social y, de ese modo, una adecuada administración de los recursos económicos por medio del Estado. Estas elucubraciones teóricas iniciaron un proceso por la socialización de los derechos fundamentales, así que, desde fines del siglo XIX hasta principios del siglo XX, en las posteriores declaraciones de derechos estos fueron los protagonistas.

Con estos nuevos conceptos jurídico-sociales, que empaparon los sistemas normativos, el individuo dejó de ser el centro de atención, desplazándose hacia la colectividad. Justamente, los constitucionalistas empezaron a observar dentro de las declaraciones de derechos dos tipos de derechos: los llamados individuales y, en contraposición a estos, los nombrados derechos sociales.

¹²²González, C. *Op. cit.*, p. 25. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 29.

Los conflictos estatales y la llamada Gran Depresión gestaron otra clase de derechos, denominados derechos de tercera generación. De orientación diferente a los anteriores, pretendían proteger a la colectividad de los daños potenciales que la misma sociedad pudiera generar a futuro. Así, en la época de la posguerra, con la decepción humana por los horrores vividos, se produjo la proclamación de derechos humanos más importante del siglo: la Declaración de los Derechos Humanos de 1948. Con ésta se dio el primer paso en el reconocimiento de la importancia de la información en la actividad humana actual y fue por esta razón que un tiempo después el Pontífice JUAN XXIII, en la encíclica *Mater et Magistra*, y la UNESCO, en sus múltiples estudios de la década de los setenta, reconocieron que la información era uno de los pilares de la sociedad moderna.

La información se conoció como el medio más eficaz en el desarrollo del mercado, de la política e, inclusive, de la guerra, pues con el auge de la llamada "Guerra Fría", los gobiernos pusieron todos sus esfuerzos en desarrollar métodos rápidos, eficaces y seguros para comunicarse, en caso de una confrontación bélica. Así, por investigaciones lideradas por la *National Security Agency* y la *Central Inteligency Agency*, de los Estados Unidos, por la K. G. B. Rusa, y por las agencias que buscaban la expansión de los horizontes territoriales como la N.A.S.A, se desarrollaron las primeras tecnologías que harían posible el viaje del hombre a la Luna y toda una serie de desarrollos en telecomunicación, como la ARPANET -ahora Internet- y las potentes comunicaciones satelitales que permiten ubicar geográficamente a los miembros de cada una de estas centrales en el mundo (MARQUEZ ESCOBAR, P. C., 2002:30)¹²³.

¹²³Cf. Witaker, Cari. (1999). *The end of privacy*. New York: The New Press. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 30.

La guerra fue madre y el capitalismo padre de la informatización, pues el desarrollo actual de las tecnologías de la informática se debe sólo a que los intereses capitalistas cortejaron a los intereses del Estado para no dejarse atrapar por los movimientos sociales ocurridos en Asia.

Así pues, con todas estas influencias, la información y la expresión, como libertades y como derechos, pasaron a ser parte integrante de la mayoría de los textos constitucionales de los Estados democráticos que dentro de tales períodos reformaron sus constituciones (MARQUEZ ESCOBAR, P. C., 2002:25-30)¹²⁴.

1.8.2. Las libertades y la Información en los Tratados Internacionales referentes a Derechos Humanos

A partir de la Declaración de los Derechos del Hombre y del Ciudadano, y en especial de la primera enmienda de la Constitución de los Estados Unidos, la libertad de expresión se convirtió en un derecho reconocido constitucionalmente. Sólo con los desarrollos de los derechos colectivos en la posguerra se reconoció el derecho de la información en un rango constitucional.

La consagración positiva demuestra el desarrollo que ha tenido la institución. Así, en los primeros textos, el bien jurídico a proteger era el de la tecnología de la información que estaba en auge, ya que la protección se centraba sobre el ejercicio de la actividad de la expresión a través de la imprenta y no sobre la expresión como bien en sí. Lo mismo sucedió al consagrar la libertad de prensa pues ésta, a pesar de ser parte integrante de la libertad de expresión,

¹²⁴ MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 25-30.

fue tomada como el modo fundamental de expresión y, por esto, debía ser protegida por las leyes y las declaraciones. Así, el texto de la Declaración de Derechos de Virginia, en su artículo 12, establece que *"la libertad de prensa es uno de los grandes baluartes de la libertad y no puede ser restringida jamás"*, demostrando esa profunda veneración a la imprenta, los pasquines y demás prácticas humanas que permitían la expresión de las ideas y el pensamiento.

Con el mismo perfil se estableció en la primera enmienda de la Constitución Norteamericana que *"el congreso no hará ley alguna por la que se establezca una religión, o se prohíba ejercerla, o se limite la libertad de palabra, o la de prensa, o el derecho del pueblo a reunirse pacíficamente y pedir al gobierno la reparación de sus agravios"* (MARQUEZ ESCOBAR, P. C., 2002:30)¹²⁵. Este texto logra un avance significativo al reconocer "la libertad de palabra", como la libertad de expresión, junto a la libertad de prensa, de manera que el texto reconocía como iguales en jerarquía, y como derechos distintos, a la libertad de palabra y la libertad de prensa.

En un sentido mucho más abierto, donde el análisis se ve influenciado por los pensamientos de los constitucionalistas europeos de la época, se presenta la Declaración Universal de los Derechos del Hombre y del Ciudadano. En ésta se estableció que *"la libre comunicación de los pensamientos y de las opiniones es uno de los derechos más preciados del hombre"* (MARQUEZ ESCOBAR, P. C., 2002:31)¹²⁶. Este texto resalta la importancia de la libertad

¹²⁵Texto citado por Desantes, José María, *op. cit.* p. 50. Para una referencia completa sobre el alcance de la libertad de expresión en la primera enmienda recomendamos la lectura de Post, Robert, "The consiitutional concept of public discourse", *Harvard Law Review*, No. 3 Vol. 103. Donde se analiza la sentencia de la Supream Court of Justice de los Estados Unidos respecto del Caso Hustler Magasine Vs. Falwell, representado en la película "the people vs. Larry Flint". Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 30.

¹²⁶Declaración universal de los derechos del hombre, *en* Constitución Política de Colombia, Santafé de Bogotá, Legls, 2000. Citado en: MÁRQUEZ ESCOBAR, P.C., *Op. Cit.*, p. 31.

de expresión para el hombre y, sobre todo, para el hombre como ciudadano. Seguidamente, define la importancia y la aplicación del derecho diciendo que *"todo ciudadano puede, por lo tanto, hablar, escribir e imprimir textos libremente, salvo la responsabilidad que el abuso de esta libertad produzca en los casos determinados por la ley"* (MARQUEZ ESCOBAR, P. C., 2002:31)¹²⁷. Esta parte del texto muestra el campo de aplicación de la libertad de expresión, es decir, trata de ejemplificar dónde se debe respetar este derecho y a través de qué tecnologías de la información, esto es, la imprenta.

De ese modo se consagraron las primeras manifestaciones internacionales sobre la libertad de expresión y sólo, casi dos siglos después, se trató de consagrar la libertad de información como mecanismo protector de los derechos de la información. Por esto, como dice DESANTES, "la libertad de expresión es por su misma naturaleza, incapaz de proporcionar al hombre un instrumento jurídicamente hábil para satisfacer su necesidad de información" (DESANTES, J. M., en MARQUEZ ESCOBAR, P. C., 2002:20)¹²⁸. Así, en la época de la posguerra, llamada por algunos la época "de los derechos humanos", se dieron los primeros textos que reconocían a la información como derecho, y en ese sentido se iniciaron los adelantos en materia de derecho de la información.

Textos como el de la Declaración Universal de los Derechos Humanos generaron los desarrollos constitucionales en el mundo a este respecto. Así, la Declaración establece en su artículo 19 que *"[Todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de*

¹²⁷*Ibíd.* Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 31.

¹²⁸Desantes,J.M., *Op. Cit.*, p. 51. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 31.

expresión". La norma contiene el primer esfuerzo por mencionar a la información como *bien* a proteger, al decir que se tiene el derecho a *investigar y recibir informaciones*, En este sentido se establece por primera vez la otra vía de la información, pues si antes sólo se pensaba desde el sujeto activo, el emisor, con la declaración se resalta la importancia del carácter pasivo de la información, es decir, la recepción. Esto no quiere decir que se haya agotado el derecho constitucional informático en estos dos caracteres pues, como lo veremos más tarde, tanto el carácter pasivo como el activo implican muchas opciones diferentes, lo que hace a los derechos de la información una aptitud humana muy rica en manifestaciones de todo tipo.

Según DESANTES, la norma mencionada no tiene obligatoriedad definida por provenir de la O.N.U., pues las únicas decisiones "obligatorias", en su verdadero sentido, son las emitidas por el CONSEJO de SEGURIDAD de este organismo. Aun así, la fuerza obligatoria directa de estas declaraciones ha sido otorgada por los tratados y convenios internacionales con relación a estos derechos. Los países miembros de la O.N.U. se han comprometido regionalmente al cumplimiento de tal cometido a partir del año 1962, cuando la organización declaró que éste era el año de los derechos humanos y que según sus artículos 55 y 56, los Estados debían hacer lo posible para que dentro de sus regulaciones se implantara una cultura de respeto a los derechos humanos (art. 55), y que tales derechos debían ser avalados mediante programas para respetar lo dicho en el artículo 55 (art. 56). Así pues, la "fuerza vinculante directa" del Derecho Internacional Humanitario sólo se consigue con los pactos internacionales, tal como lo señala DESANTES (MARQUEZ ESCOBAR, P. C., 2002:20)¹²⁹.

Posteriormente, los pactos internacionales y regionales de Derechos Humanos se pusieron a la orden del día, de modo que el 16 de diciembre de

¹²⁹Desantes, J.M., *Op. cit.*, p. 54. Citado en: MÁRQUEZ ESCOBAR, P.C., *Op. Cit.*, p. 32.

1966 se promulga el *Pacto Internacional de Derechos Civiles y Políticos*, quizá el más importante de todos, ya que fue suscrito por todos los países miembros de la O.N.U. Este pacto manifiesta en su artículo 19 que "*nadie podrá ser molestado a causa de sus opiniones*" y, además, que *toda persona tiene derecho a la libertad de expresión, comprendida la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea de manera oral, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*"¹³⁰. El texto comprueba por sí mismo la evolución con respecto al aprobado en el seno de la llamada *Declaración Internacional de los Derechos Humanos*, pues demuestra inicialmente una tendencia hacia la clasificación de información como parte de la libertad de expresión, actitud con la que no estamos de acuerdo teóricamente por motivos que expresaremos al hacer el análisis del texto de nuestra Constitución. De cualquier modo, es destacable el desarrollo debido a que el esfuerzo teórico pretendía abarcar todas las conductas informáticas del hombre, tanto las pasivas como las activas, ya que al decir "buscar, recibir y difundir informaciones" se ilumina esa actitud humana activa de investigar y expresar, y la actitud pasiva ante la facultad informativa de los demás, facultad que incluye responsabilidades. Estos últimos textos internacionales demuestran que la libertad de expresión se desligó de las tecnologías de la información, pues se creó un concepto informático independiente de los medios informáticos con la declaración de la existencia del derecho, sin importar el medio informático utilizado para la realización del mismo. Desde cierto punto de vista, se puede decir que el texto mencionado se inspiró en categorías *puras* (MARQUEZ ESCOBAR, P. C., 2002:33)¹³¹.

¹³⁰Pacto Internacional de Derechos Civiles y Políticos. Artículo 14 de la Ley 74 de 1968. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 32.

¹³¹Los anteriores textos demostraban un profundo desconocimiento de lo que es el concepto y su diferencia con los efectos del concepto. En ellos se asignaba el derecho no sólo por pertenecer al grupo protegido, sino también por ser efecto de lo protegido. Esto es claro al analizar la libertad de expresión con respecto a la libertad de prensa, que son libertades jurídicamente independientes pero teóricamente consubstanciales, pues la libertad de prensa se desprende de los fenómenos que comprenden la libertad de expresión, pero ella no agota

Luego de este pacto, quizá por su importancia territorial reducida, se dio, en el ámbito europeo, la *Convención Europea de Salvaguardia de los Derechos Humanos y de las Libertades Fundamentales*, nacida el 4 de noviembre de 1950, en el seno del Consejo de Europa. Cuenta con una Comisión y un Tribunal con competencia, llegado el caso, para proceder al examen y la resolución de conflictos relacionados con la vulneración de los derechos y libertades contenidos en la Convención.

Después, en el ámbito americano se gestó el *Pacto de San José de Costa Rica*, nombrado oficialmente como *Convención Americana sobre Derechos Humanos*, que sin un esfuerzo por repensar tales derechos, a partir de los estudios publicados en la época, adoptó el mismo texto del artículo 14 del *Pacto internacional de los Derechos Civiles y Políticos* en el artículo 13¹³².

1.8.3. La información en el ámbito del Derecho Constitucional mundial

El análisis del desarrollo histórico-jurídico de la libertad de expresión y la libertad de información nos da una de las primeras conclusiones de este capítulo. El estudio nos demostró que tales libertades y su evolución coinciden con el desarrollo y evolución de las instituciones democráticas occidentales, de

la libertad de expresión por ser ésta formada por un cúmulo de manifestaciones diferentes a la simple prensa. Aclaramos que al analizar la libertad de información con respecto a la libertad de expresión sucede lo mismo que a ésta con la libertad de prensa, pues la libertad de información es uno de los fenómenos informáticos, que no agota las libertades informáticas aunque las dos sean fruto de esa tan feliz cualidad humana llamada autodeterminación. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 33.

¹³²Convención Americana sobre Derechos Humanos. Pacto de San José. Artículo 13. Ley 16 de 1972. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 33.

manera tal que se convierten tales libertades, cada una en su etapa, en uno de los principios de la institución democrática. En este sentido planteamos el análisis del derecho constitucional comparado, puesto que cada Estado, según su inclinación a la democracia liberal o social, o a otro régimen político, plantea las libertades informativas de diferentes maneras en su Constitución.

El catedrático español VILLANUEVA VILLANUEVA, en su libro *Derecho comparado de la información* (VILLANUEVA, E. en MARQUEZ ESCOBAR, P. C., 2002:20)¹³³, en el capítulo primero, efectúa un análisis del derecho constitucional comparado de las libertades de expresión e información. Para él existen seis tipologías de sistemas constitucionales en materia de libertades informativas" (Villanueva, E., en MARQUEZ ESCOBAR, P. C., 2002:20)¹³⁴. Esta clasificación se hace según la cantidad de disposiciones constitucionales que tiene cada estatuto, en cuanto a las libertades y derechos informativos se refiere. Inicia con una mención del porcentaje de países (Israel Lesotho, Ornan y San Marino en MARQUEZ ESCOBAR, P. C., 2002:34)¹³⁵ que no recogen disposiciones constitucionales al respecto, sea o porque no tienen Constitución o porque en ella no se dice nada respecto de las libertades. En segundo lugar aparece un sistema denominado por VILLANUEVA como *improtección*, pues estos países (MARQUEZ ESCOBAR, P. C., 2002:34)¹³⁶ "no reconoce[n] -en su Constitución- ninguna de las libertades informativas, o delega su establecimiento y protección a una ley orgánica o reconociéndolas, sujeta su ejercicio a restricciones más allá de las taxativamente previstas en

¹³³Villanueva Villanueva, Ernesto, *Derecho Comparado de la Información*, México, Universidad Iberoamericana, 1988. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 33.

¹³⁴*Ibid.*, p. 35. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 34.

¹³⁵En esta categoría están Australia, Gran Bretaña, Israel, Lesotho, Ornan y San Marino. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 34.

¹³⁶Se encuentran dentro de este rubro Arabia Saudita, Birmania, Brunei, Camerún, Costa de Marfil, Cuba, Irán, Iraq, Libia, Omán, Paquistán, Qatary Yemen. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 34.

la ley" (MARQUEZ ESCOBAR, P. C., 2002:34)¹³⁷. En tercer lugar reconoce el sistema denominado *Decimonónico*, en el cual la Constitución de estos países (MARQUEZ ESCOBAR, P. C., 2002:34)¹³⁸ establece genéricamente las libertades de expresión, de prensa e imprenta y donde el papel del Estado es pasivo, de modo que tiene un deber de abstención. En cuarto lugar tenemos el sistema *Minimalista*, en el cual los países (MARQUEZ ESCOBAR, P. C., 2002:34)¹³⁹ reconocen en su Constitución "*además de las libertades de expresión e imprenta, la libertad de información, mediante la cual se dota al individuo de la posibilidad de que cuente con los elementos mínimos para participar de la res publica*" (Villanueva en MARQUEZ ESCOBAR, P. C., 2002:34)¹⁴⁰. En quinto lugar está el sistema llamado *cuasi-paradigmático* (MARQUEZ ESCOBAR, P. C., 2002:34)¹⁴¹ en el cual se reconocen las libertades informativas, y dos de las figuras jurídicas siguientes: el derecho de réplica, el derecho de acceso a los documentos públicos, el secreto

¹³⁷Villanueva Villanueva, Ernesto, *Op. Cit.*, p. 35. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 34.

¹³⁸Los países que recogen este tipo de disposiciones son: Afganistán, Angola, Argelia, Argentina, Bahrein, Bangladesh, Bélgica, Benin, Bolivia, Burkina Faso, Burundi, Camboya, Canadá, Comoras, Corea, Corea del Norte, Costa Rica, Chechenia, China, Dinamarca, Djibouti, Egipto, El Salvador, Emiratos Árabes Unidos, Francia, Grecia, Guatemala, Guinea, Guinea-Bissau, Guinea Ecuatorial, Haití, Honduras, India, Indonesia, Irlanda, Islandia, Italia, Japón, Jordania, Krajina, Kuwait, Laos, Líbano, Liberia, Liechtenstein, Luxemburgo, Madagascar, Malasia, Malawi, Malí, Mauritania, Marruecos, México, Moldavia, Mónaco, Namibia, Nauru, Nepal, Níger, Países Bajos, Panamá, Polonia, Puerto Rico, República Africana Central, República Dominicana, Ruanda, Samoa Occidental, Santo Tomas y Padre, Senegal, Singapur, Siria, Somalia, Sri Lanka, Sudan, Suiza, Surinam, Tayikistán, Tonga, Trinidad y Tobago, Túnez, Turquía, Ucrania, Uganda, Uruguay, Vanuatu, Venezuela, Vietnam y Zaire. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, P. 34.

¹³⁹Según el autor se encuentran en este grupo Alemania, Albania, Antigua, Austria, Azerbaiyán, Bahamas, Barbados, Belice, Botsuana, Congo, Chad, Chipre, Dominica, Etiopía, Fiji, Filipinas, Finlandia, Kenia, Kiribati, Kyrghystan, Letonia, Malta, Mauricio, Mongolia, Nigeria, Nueva Zelanda, Papua Nueva Guinea, San Christopher y Nevis, San Vicente, Santa Lucía, Seychelles, Sierra Leona, Suazilandia, Sudáfrica, Tanzania, Togo, Turquemenistan, Tavalu, Zambia y Zimbabue. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, P. 34.

¹⁴⁰Villanueva Villanueva, Ernesto, *Op. Cit.*, p. 36. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 34.

¹⁴¹Dentro de este grupo se encuentran Bielorusla, Bosnia-Herzagovina, Bulgaria, Chile, Ecuador, Estonia, Kasakhastán, Lituania, Montenegro, Mozambique, Nicaragua, República Checa, Rumania, Rusia, Serbia, Tailandia, Uzbequistán y Yugoslavia. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.34.

profesional, la cláusula de conciencia y el derecho de autor del trabajo periodístico. Además, en estos sistemas se reconoce un papel activo y pasivo del Estado, de tal manera que las libertades informativas se convierten en punto fundamental para el desarrollo de la democracia. Para finalizar encuentra el sistema *paradigmático* (MARQUEZ ESCOBAR, P. C., 2002:34)¹⁴², el cual comprende las libertades informativas y tres de las figuras informativas destacadas en el sistema anterior, además de un papel activo del Estado más profundo para el ejercicio de las libertades y para la protección del individuo en la injerencia de los entes públicos y de otras entidades sociales con la capacidad de "impedir la formación de una opinión pública libre". (MARQUEZ ESCOBAR, P. C., 2002:35)¹⁴³

De este modo el autor concluye con un análisis estadístico cada sistema, demostrando que el más recurrido por las constituciones es el *Decimonónico*, pues un 48% de los países lo tienen. Luego le siguen el *minimalista* con un 25%, el *cuasi paradigmático* con un 9%, el *improtectivo* y el *paradigmático* empatan con un 7% y, en último lugar, los que no tienen previsiones constitucionales con un 4%.

El estudio que acabamos de mostrar es muy completo, debido a que recoge el texto referente a las libertades informativas de las constituciones de cada país, además de hacer el análisis estadístico de cada una de las libertades y de los sistemas. Aun así, creemos que el estudio podría haber sido más completo teóricamente si mostrara las tendencias regionales y las aplicaciones de las libertades informáticas según el sistema de gobierno y el tipo de régimen político de cada uno de estos Estados.

¹⁴²Pertenecen a esta categoría los países de Andorra, Brasil, Cabo Verde, Colombia, Croacia, Eslovaquia, Eslovenia, España, Hungría, Macedonia, Paraguay, Perú, Portugal y Suecia. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogotá D.C.: Leyer, p. 35.

¹⁴³Villanueva Villanueva, Ernesto, *Op. Cit.*, p. 37. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogotá D.C.: Leyer, p.35.

Además, en países como los Estados Unidos, el hecho de clasificarse en el sistema *deciminónico* hace que se dude un poco de la integridad de la investigación, pues parece sólo haberse fijado en el texto constitucional y no en el sistema de precedentes judiciales que, como todos conocemos, *amplían* las normas de los sistemas anglosajones y de algunos países continentales (MARQUEZ ESCOBAR, P. C., 2002:35)¹⁴⁴.

Para ampliar más este punto de vista acerca del desarrollo de la democracia y de los sistemas basados en los principios de la tolerancia y el pluralismo con la evolución de las libertades informáticas, vamos a continuar con el análisis de los textos constitucionales de algunos países para mostrar la influencia del sistema y el régimen político en el desarrollo y respeto de las libertades informáticas. Para hacer este examen procederemos analizando el texto de países con cada uno de los sistemas descritos por VILLANUEVA.

En el sistema *Improtectivo*, encontramos Estados conocidos por sus inclinaciones religiosas o políticas. Es el caso de Pakistán y Cuba. Pakistán es "una República islámica con sistema de gobierno federal", sistema que se restableció después del Golpe de Estado y en el que, en 1991, se concordó que todas las leyes cumplieran con las obligaciones de la *sharia* -ley islámica. La influencia del Islamismo en la Constitución Pakistaní se ve reflejada en todas sus mormas. Así, en las disposiciones que estamos estudiando no hay excepción, el texto refleja la importante influencia y limitaciones que el Islam a través del Corán ha producido. El texto dice:

"Artículo 14. (1) La dignidad del hombre y, sujeto a la ley, la privacidad de su hogar serán inviolables.

¹⁴⁴Un análisis detallado lo encontramos en López, Diego, *El valor del precedente judicial*, en *Observatorio de Justicia Constitucional*. Santafé de Bogotá. Siglo del Hombre. 1998. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.35

“Artículo 19. Todo ciudadano tendrá el derecho a la libertad de palabra y de expresión, y habrá libertad de prensa, sujeta a restricciones razonables establecidas por la ley en el interés de la gloria del Islam o de la integridad, seguridad y defensa de Paquistán o cualquiera de sus partes, en relaciones amistosas con Estados extranjeros, el orden público, la decencia o la moralidad o en relación al desacato de la Corte o la Incitación a cometer delitos”¹⁴⁵.

Es claro en el texto que el interés a proteger no es la democracia, ni los principios democráticos mencionados, lo importante es la defensa del Islam y el Estado Paquistaní. Las libertades se encuentran con una talanquera del tamaño del Corán, de manera que se coarta a la prensa, quienes siendo el principal medio de difusión de información pierden, por decirlo así, la libertad de expresión.

Por su parte, el texto de la Constitución cubana tiene el mismo perfil que la Constitución paquistaní, pero su orientación limitativa se da de modo que lo que busca proteger el texto constitucional no es la religión o la moral pero sí un ideal político, el socialismo. De esta manera el reconocimiento de las libertades se da sólo en razón a los fines de la sociedad socialista, y como dice el texto constitucional, en su artículo 52:

"las condiciones materiales para su ejercicio están dadas por el hecho de que la prensa, la radio, la televisión, el cine y otros medios de difusión masiva son de propiedad estatal o social y no pueden ser objeto, en ningún caso, de propiedad privada, lo que asegura

¹⁴⁵Constitución de República Islámica de Pakistán, adoptada el 12 de abril de 1973. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.36.

su uso al servicio exclusivo del pueblo trabajador y del interés de la sociedad" (MARQUEZ ESCOBAR, P. C., 2002:35) ¹⁴⁶.

En el sistema *Decimonónico* encontramos países con un alto grado de desarrollo de las libertades informativas, como es el caso de los Estados Unidos, países para los que sus textos constitucionales se quedaron cortos hace tiempo, y su sistema legal ha reemplazado, a través de decisiones judiciales o leyes, tales falencias constitucionales. Aun así, se encuentran otros en que el desarrollo tardío de sus sistemas políticos no ha hecho posible una consagración completa de las libertades informativas. En el caso de China, la Constitución establece la garantía constitucional de la libertad de expresión y las libertades asociativas, y en contra de la percepción general no impone ninguna limitación al ejercicio no violento de dichas libertades (MARQUEZ ESCOBAR, P. C., 2002:37) ¹⁴⁷.

También sucede algo parecido con Estados como Uruguay en donde, a diferencia de los demás Estados suramericanos, exceptuando Venezuela, se da un texto constitucional que no es muy acorde con las tendencias de la época, pero que resalta el poco desarrollo que tienen en el papel las libertades informativas dentro de la también, no muy desarrollada, democracia. En Venezuela se dio un caso parecido, pues para la época de la adopción de la Constitución venezolana no se había acentuado profundamente el desarrollo de las libertades informativas democráticas, de modo que el texto constitucional adopta la libertad de expresión, al igual que lo hace Uruguay, pero con una técnica legislativa superior, pues desarrolla el contexto del derecho dentro de la misma disposición. Ahora su texto constitucional es de corte minimalista debido a que establece que la comunicación es libre y plural,

¹⁴⁶Constitución de la República Socialista Cubana, adoptada en 1959 y reformada en 1992. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.36.

¹⁴⁷Constitución de la República Popular China, adoptada el 14 de diciembre de 1982. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 37.

y toda persona tiene derecho a la información oportuna, veraz e imparcial, sin censura, de acuerdo con los principios de esta Constitución (MARQUEZ ESCOBAR, P. C., 2002:37)¹⁴⁸.

En los sistemas *Minimalista*, *Cuasi paradigmático* y *Paradigmático* se encuentran una infinidad de países que por su formación, sistema de gobierno, forma de Estado y adopción constitucional favorecen a la democracia liberal y, de paso, a las libertades informativas que últimamente están siendo incluidas en los catálogos de derechos de las constituciones de los países con democracias sólidas y en desarrollo (MARQUEZ ESCOBAR, P. C., 2002:33-37)¹⁴⁹.

1.8.4. La información en el Constitucionalismo Colombiano

Para comenzar, al igual que lo hicimos en el anterior acápite, vamos a darle un breve vistazo a la evolución que en Colombia ha tenido el derecho a la información en el ámbito constitucional.

Superado el período denominado del Olimpo Radical, viene la Constitución de NÚÑEZ y CARO en 1886. En ésta, por ser una Constitución conservadora, se limitó de nuevo el derecho a la libertad de expresión y de prensa. Así, la Constitución, en su artículo 42 dijo que la prensa *"es libre en tiempo de paz; pero responsable con arreglo a las leyes"*. Aun así, se estableció en esta Constitución el controversial artículo k transitorio, el cual determinó que

¹⁴⁸Constitución de la República Bolivariana de Venezuela, fuente: Global Legal Infomation, en Internet: <http://www.loc.gov>. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 37.

¹⁴⁹ MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 33-37.

"mientras no se expida la ley de imprenta el gobierno queda facultado para prevenir y reprimir los abusos de la prensa", dándose así un poder excepcional al ejecutivo de represión sobre la expresión impresa. Luego del texto constitucional de 1886 no se dieron cambios a las libertades mencionadas en las reformas de 1910, 1936, 1945, ni en el plebiscito de 1957, ni en la reforma de 1968 (MARQUEZ ESCOBAR, P. C., 2002:37-39)¹⁵⁰.

1.8.4.1. La información en la Constitución Colombiana de 1991

Después de los procesos de paz adelantados por el Gobierno BETANCUR en los años ochenta con los grupos revolucionarios y la frustrada guerra contra los carteles de la droga, que llegó a su punto más bajo con la muerte de Luis CARLOS GALÁN, el sentimiento de reforma constitucional no dio espera. El desarrollo de la séptima papeleta y el movimiento estudiantil concomitante, dieron fuerza, en el año 1990, a la reforma de la Constitución de 1886. No valieron las demandas de inconstitucionalidad del proceso de reforma ante la Corte Suprema de Justicia para detener esta causa.

En mayo de 1991 se eligieron los Constituyentes y en pocos meses se publicaría nuestra nueva Carta Política. Sus reformas a la Constitución de 1886 fueron de todo tipo. Se introdujeron nuevas figuras políticas y jurídicas, y se incluyeron en la Carta múltiples artículos tomados de los textos de los tratados internacionales, que en materia de derechos humanos había suscrito el país. Tal es el caso tema de estudio, las normas internacionales que en materia de derechos humanos suscribió Colombia en Declaración Universal de los Derechos Humanos de 1948, el Pacto de Derechos Civiles y Políticos

¹⁵⁰ MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 37-39.

aprobado en Colombia en 1968 y la Convención Americana de Derechos Humanos o Pacto de San José de Costa Rica aprobada en 1972, fueron la fuente principal de los textos constitucionales de las normas sobre derechos fundamentales. Y habían de serlo, pues era la mejor manera de demostrar el compromiso del país con los pactos y tratados internacionales de Derecho Internacional Humanitario.

El derecho a la libertad de opinión, expresión y de información fue consagrado en el artículo 20 de la Carta, cuyo tenor establece que *"[s]e garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación"* (MARQUEZ ESCOBAR, P. C., 2002:40)¹⁵¹.

En el debate constituyente sobre la norma mencionada, el constituyente RAMÍREZ OCAMPO hizo un análisis de la norma propuesta en comparación con la que se modificaba (art. 42 Constitución de 1886), diciendo que el nuevo texto ampliaba la norma constitucional anterior, pues incluía el derecho a informar y ser informado y el derecho, conexo con el anterior, de fundar medios masivos de comunicación como desarrollo de la libertad de expresión y de pensamiento¹⁵². Así pues, podemos decir que a partir del nuevo texto, inspirado en el ya mencionado artículo 13 de la Convención Americana sobre Derechos Humanos, se fundamentan en la Constitución los derechos a la información, expresión y opinión.

Respecto de este derecho, los constitucionalistas colombianos no han tenido muchos reparos, puesto que para estos el texto obedece a la correcta

¹⁵¹Gaceta Constitucional No. 127, p. 3. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 40.

¹⁵²Gaceta Constitucional No. 112, p. 7, citado por Lleras de la Fuente, Carlos; Tangarife Torres, Marcel. (1996). *Constitución Política de Colombia. Origen, evolución y vigencia*, Santafé de Bogotá: Diké. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 40.

clasificación lógica de las libertades. Tal es el caso de NARANJO, para quien éstas son tres libertades autónomas e independientes según lo establece en su texto *Teoría Constitucional e Instituciones Políticas*, haciéndolas parte del grupo de las libertades intelectuales, de manera que comparten su género próximo con la libertad de enseñanza y con una libertad, denominada por él, de telecomunicaciones que se refiere a la libertad de fundar medios de comunicación, la cual en nuestra opinión no es más que una variante de la libertad de empresa.

También aparece dentro de este tipo de catedráticos Luis CARLOS SÁCHICA, quien parece tomar muy a pecho el tema y critica con algo de razón el texto constitucional, al decir que éste no hace referencia a quien debe responder por informar y recibir información veraz e imparcial. Claro que como el sujeto del texto constitucional es indeterminado, es obvio que el emisor de la información puede ser cualquiera, para eso está la ya mencionada libertad de fundación de medios comunicativos (MARQUEZ ESCOBAR, P. C., 2002:40)¹⁵³.

Luego del análisis de medio párrafo que le dedica el anterior tratadista al artículo mencionado, tenemos la interpretación de HENAO HIDRÓN para quien tampoco es importante el tema y decide simplemente hacer una mención en un párrafo, al decir que ésta es una de las libertades consagradas dentro del capítulo de los derechos fundamentales de la Constitución (MARQUEZ ESCOBAR, P. C., 2002:41)¹⁵⁴.

¹⁵³Sáchica, Luis Carlos. (1992). *Nuevo constitucionalismo colombiano*, Santafé de Bogotá: Temis, p. 209. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 40.

¹⁵⁴Henao Hidrón, Javier. (1992). *Panorama del derecho constitucional colombiano*, Santafé de Bogotá: Temis, p. 185. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 41.

También se inscribe en la tendencia que estamos tratando el autor MENDOZA PALOMINO, quien desde un punto de vista al parecer psicológico, encuentra que las libertades de opinión, expresión e información hacen parte de un conjunto de derechos individuales que propenden por la búsqueda de la integridad de la personalidad. Dentro de las libertades, divide las de expresión y las de información por ser interdependientes unas de otras, pero les hace compartir su género por ser libertades, junto a las libertades de enseñanza y las libertades espirituales; todas inscritas aún dentro de las normas protectoras de la personalidad del individuo (MARQUEZ ESCOBAR, P. C., 2002:41)¹⁵⁵.

También encontramos loable mencionar la clasificación que hace MADRID-MALO de los derechos fundamentales, al establecer unas libertades llamadas de la comunicación, dentro de las cuales se encuentran las libertades de expresión, difusión e información. No se encuentra la libertad de opinión, pues el autor considera que ésta debe diferenciarse de las libertades de pensamiento y de las libertades de comunicación, puesto que, a pesar de que todas responden a la racionalidad humana, la primera, la de pensamiento, no implica necesariamente un acto mental de opinión, y la de expresión, surge como presupuesto para el desarrollo de las libertades de comunicación, ya que sin la opinión éstas no tienen validez. El autor también recalca que antes de la opinión está la autonomía que es, para nosotros, la vértebra que sostiene los derechos individuales. Así el autor encuentra que primero está la autonomía como cabeza y de ella se desprenden características del hombre como el pensamiento, del cual se desliga la opinión y, a partir de ésta, las libertades comunicativas (MARQUEZ ESCOBAR, P. C., 2002:41)¹⁵⁶.

¹⁵⁵Mendoza Palomino, Alvaro. (1992). *Teoría y Sinopsis de la Constitución de 1991*, Santafé de Bogotá: Doctrina y Ley, p. 245 y ss. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p. 41.

¹⁵⁶Madrid-Malo, Mario. (1995), *Estudios sobre derechos fundamentales*, Santafé de Bogotá: Tercer Mundo. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.41.

Al parecer, la teoría que presenta un mejor sustento filosófico, jurídico y constitucional es la del Catedrático MADRID-MALO, pues es coherente en tanto que demuestra un orden jerárquico dentro de la "naturaleza humana" y dentro de la característica que el autor menciona como la principal del hombre, su racionalidad. Aun así, dicha teoría adolece de un defecto en tanto en cuanto considera, al igual que NARANJO, que la libertad de difusión o de fundar medios masivos de comunicación es una libertad independiente de la libertad de información, siendo que es una manera de desarrollar el derecho y la libertad de informar frente de la libertad de empresa. Esto hubiese sido más coherente, si el texto constitucional aprobado dentro de la comisión primera de la constituyente, hubiere sido el primero presentado, el cual finalizaba en su primer inciso diciendo que *"los derechos de informar y de opinar comprenden los de fundar medios masivos de comunicación"* (MARQUEZ ESCOBAR, P. C., 2002:41)¹⁵⁷. Redactado de esta manera, la información y la opinión se entenderían como el sustento de la fundación de medios masivos de comunicación, pues de seguro, si se limita el derecho a informar y ser informado, de nada sirve el fundar medios masivos de comunicación, ya que estos son canales de transmisión de datos.

Para pensar los derechos fundamentales de la comunicación hemos de partir de la teoría de la información antes dada, diciendo que como principio rector de estas tenemos la autonomía de las prácticas humanas. Así pues, de la autonomía surge la libertad de pensamiento, de la cual a su vez surge la libertad de opinión y de ésta se tiene toda libertad de información. Esta última se desenvuelve de dos modos: uno como facultad humana para recibir información y otro como práctica humana para difundir información. Para la difusión de la información es necesario tener la libertad de expresión, para el

¹⁵⁷Gaceta Constitucional No. 83, Bogotá, Imprenta Nacional, 1991. Citado en: MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, p.41.

mejor desarrollo de ésta, se da la libertad de fundación de medios masivos de comunicación teniendo en cuenta que está limitada por la veracidad e imparcialidad de la información (MARQUEZ ESCOBAR, P. C., 2002:39-42)¹⁵⁸.

1.8.4.1.1. Desarrollo legislativo y jurisprudencial en materia de información y datos en Colombia

Con ocasión del XV Congreso Iberoamericano de Derecho e Informática. Organizado por la Federación Iberoamericana de asociaciones Derecho e informática (FIADI). Celebrada en Buenos Aires, Argentina del 3 al 8 de octubre de 2011, tuvimos la oportunidad de presentar una sinopsis de la experiencia colombiana en la materia, bajo el título: DE LO LEGISLATIVO A LO JURISPRUDENCIAL EN MATERIA DE CIBERDELINCUENCIA EN COLOMBIA (RINCÓN RÍOS, J. y NARANJO DUQUE, V. 2013)¹⁵⁹, la cual consideramos de mucho provecho y pertinencia en el marco del presente trabajo investigativo.

El auge de la sociedad de la información, impulsado por el desarrollo de las tecnologías hace gala en el escenario jurídico colombiano, lo mismo que en América Latina. En los últimos cinco años, se ha dado un desarrollo vertiginoso legislativo y jurisprudencial en materia digital, todo a partir de los debates doctrinales y académicos que se han venido dando en los diferentes escenarios nacionales e internacionales.

¹⁵⁸MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer, pp. 39-42.

¹⁵⁹Síntesis del libro *"Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia."* RINCÓN RÍOS, J. y NARANJO DUQUE, V. (2013) *"Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia."* Bogota D.C.: IBAÑEZ Editores. Primera reimpresión a la 1° Edición.

En Colombia, la protección a la información, empieza a materializarse principalmente con la aprobación de la Ley 1266 de 2008, Ley de Habeas Data y manejo de información contenida en bases de datos personales, declarada exequible por la Honorable Corte Constitucional en su sentencia C-1011 de 2008, pronunciamiento en el que se define el contenido esencial del derecho fundamental al Habeas Data, estableciendo que éste *“radica en el ejercicio efectivo, por parte del sujeto concernido, de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en archivos y bancos de datos.”* A partir de este momento se visualiza en el contexto legislativo y jurídico nacional, un desarrollo sin precedentes en cuanto a la salvaguarda y protección de la información.

Partiendo de este punto, se logra concretar la inclusión de “La información y los datos” dentro de los bienes jurídicos tutelados que protege el legislador a través de la Ley Penal. Es así como el 5 de enero del año 2009, por fin se sanciona la Ley 1273 de Delito Informático en Colombia, “Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”, siendo un avance significativo por cuanto reconoce la categoría de bien jurídico tutelado a la información y/o el dato, introduciendo su protección al ámbito penal, equiparando la legislación colombiana a los mayores desarrollos legislativos en la materia a nivel mundial, creando 9 tipos penales nuevos dentro del Código Penal Colombiano Ley 599 de 2000, para la protección de la información y los datos, sino también agregando como circunstancia de mayor punibilidad en el artículo 58 de la parte general del Código Penal, el numeral 17 que reza: *“Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos”*, circunstancia que permite un aumento de pena para la comisión

de cualquier tipo penal que se valga de dichos medios para vulnerar bienes jurídicos protegidos.

Los nuevos tipos penales y sus circunstancias de agravación punitiva son agrupados en un nuevo Título dentro del Código Penal, el Título VII Bis “De la protección de la información y de los datos”, que se encuentra dividido en dos capítulos, el primero denominado *“De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”* donde se penalizan con privación de la libertad y multa los delitos de: Acceso abusivo a un sistema informático (Art. 269A C.P.), Obstaculización ilegítima de sistema informático o red de telecomunicación (Art. 269B C.P.), Interceptación de datos informáticos (Art. 269C C.P.), Daño informático (Art. 269D C.P.), Uso de software malicioso (Art. 269E C.P.), Violación de datos personales (Art. 269F C.P.) y Suplantación de sitios web para capturar datos personales (Art. 269G C.P.). Y el segundo, denominado *“De los atentados informáticos y otras infracciones”* donde se penalizan, también con privación de la libertad y multa los siguientes delitos: Hurto por medios informáticos y semejantes (Art. 269I C.P.) y Transferencia no consentida de activos (Art. 269J C.P.).

La citada circunstancia de mayor punibilidad que agregó la Ley 1273 de 2009 (*“Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”*), al artículo 58 del Código penal en el numeral 17 ha permitido la persecución penal, investigación y juzgamiento de diferentes delitos, que aunque su naturaleza no sea de tipo informático, los medios que utilizan si lo son. Y en esta categoría recaen delitos contra el patrimonio económico, contra la libertad e integridad sexuales, contra los derechos de autor, contra la libertad individual y otras garantías. Lo que permite que en

Colombia, se reconozcan penal y judicialmente las dos categorías de delitos cibernéticos resultantes de los estudios de la Organización de las Naciones Unidas y el Consejo Europeo para delitos de alta tecnología: El primero, **Delito cibernético en sentido estricto** (“delitos informáticos”): todo compartimiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y de los datos procesados por ellos; y el segundo, **Delito cibernético en sentido lato** (“delito relacionado con computadoras”): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos”¹⁶⁰. (RINCÓN RÍOS, J. 2013)

Otra característica importante de nuestra Ley de Delitos informáticos (*Ley 1273 de 2009 “Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*”), es que recogió plenamente las recomendaciones de la Convención de Budapest del año 2001, definiendo incluso competencias, radicándola en nuestro caso en cabeza de los Jueces penales municipales según el numeral 6° del artículo 37 de la Ley 906 de 2004 Código de Procedimiento Penal, superando de esta manera el debate entre delitos contra el Patrimonio Económico y delitos Informáticos, ratificando la Corte Suprema de Justicia en Proceso Radicado N° 34564 Sala de Casación Penal. M.P. José Leonidas Bustos Martínez, que cuando estos entran en contradicción, conocen los Jueces penales

¹⁶⁰ Naciones Unidas, Décimo Congreso de las Naciones Unidas sobre la Prevención del Delito y Tratamiento del Delincuente, Viena, 10 al 17 de abril de 2000, Delitos relacionados con las redes informáticas, A/CONF.187/10, p. 5. http://www.unodc.org/pdf/crime/10_commission/resumed_session/14s.pdf, Página consultada marzo de 2007. Citado en RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez

municipales sin importar la cuantía; simplemente la naturaleza digital del ilícito claramente determinada, por la clara competencia funcional determinada en la ley.

Sin embargo, a pesar de los grandes avances y el desarrollo legislativo obtenido a partir de la Ley 1273 de 2009 (*“Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”*), existieron grandes obstáculos en su proceso de aprobación, que se reflejan en su contenido actual. En primer lugar, debemos decir que el proyecto inicial de Delitos informáticos, proyecto de ley números 042/07 Cámara, acumulado con el 123/07 Cámara “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado “de la protección de la información y de los datos”— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”, tal y como fue aprobado por la Cámara de Representantes, incluía en su artículo primero un glosario que permitiría la correcta interpretación de la ley, evitando vacíos y teniendo en cuenta que los términos utilizados en los sistemas informáticos y electrónicos no pertenecen al uso común de toda la sociedad; fueron eliminados todos los términos en inglés cuando el lenguaje que describe las conductas informáticas es mundialmente conocido en ese idioma y por último, no se elevaron a la categoría de tipo penal diferentes conductas que resultan lesivas para los bienes jurídicos tutelados que se busca proteger y que en diferentes legislaciones en el mundo si constituyen delito, como lo son: *El espionaje informático*, conducta que pretende proteger la información privilegiada industrial, comercial, política o militar relacionada con la seguridad del Estado. Se castiga, pues, la falta de sigilo o confidencialidad de los profesionales, responsables o encargados de los ficheros de los datos automatizados; *El Bloqueo ilegítimo a sistemas*

informáticos, esta conducta busca impedir el acceso a los sistemas informáticos; este comportamiento se conoce también como extorsión informática, pues el delincuente bloquea, asedia, o acorrala el sistema hasta cuando no se le cancele una suma de dinero; *Abuso de uso de medios informáticos*, este comportamiento prevé como punible el abuso de medios informáticos, mediante la introducción de verbos rectores como "intercepte", "interfiera", "use" o "permita que otro use". Ello, es consecuencia de que en materia de delitos informáticos es frecuente que el *hacker* al realizar otras conductas informáticas, ingrese abusivamente al sistema informático, por lo cual suele realizar un concurso de conductas punibles. Aquí se incluye el abuso de spam, flagelo informático que ha generado problemas económicos a los usuarios del correo electrónico, vulnerando también derechos fundamentales como el de la intimidad virtual y el hábeas data a los usuarios de la Internet y de las telecomunicaciones; *Estafa informática*, se refiere a la estafa electrónica, la que no puede ser subsumida en la estafa clásica, pues los verbos rectores son diferentes; en efecto, debe recordarse que en aquella (la clásica), la inducción se realiza en humano, en cambio en el delito informático no se puede inducir o mantener a otro en error por medio de artificios o engaños, pues las máquinas no son susceptibles de inducción al error, pues se debe manipular la información para lograr la transferencia de activos en forma ilegal. En principio, esta conducta se ha considerado como un *modus operandi*. Debe, pues, distinguirse el comportamiento de estafa logrado a través de medios informáticos, de la estafa electrónica que se refiere a la modificación de la información económica o patrimonial; *Falsedad Informática*, la tipificación de esta conducta pretende proteger todo tipo de documentos privados o públicos, que tengan carácter probatorio. Hoy, la mayoría de las transacciones en comercio electrónico se hace en este formato y son muy pocas las oportunidades que se registran en soporte papel. Piénsese, por ejemplo, en la transacción que realiza un comerciante Colombiano con zapatos Italianos y, a través de accesos ilegales al sistema,

logra modificar las condiciones de la transacción; por ejemplo, que el vendedor asuma el IVA, los valores de la transacción, que modifique el catálogo de productos, etc; y *el Spam*, cuya reglamentación en la legislación en Colombia se limita al Decreto Reglamentario 1524 de julio de 2002, donde se encuentra definido en su artículo 2° así: *“Spamming: El uso de los servicios de correo electrónico para difundir mensajes no solicitados de manera indiscriminada a una gran cantidad de destinatarios.”*. Y posteriormente en el artículo 6° del mismo decreto, se definen las medidas técnicas y administrativas, según las cuales, en su numeral primero *“Los ISP, proveedores de servicio de alojamiento o usuarios corporativos deberán implementar sistemas internos de seguridad para su red, encaminados a evitar el acceso no autorizado a su red, la realización de spamming, o que desde sistemas públicos se tenga acceso a su red, con el fin de difundir en ella contenido relacionado con pornografía infantil.”* El más cercano avance en la legislación colombiana para la regulación del Spam, fue el Proyecto de Ley N° 142 de 2004 "POR MEDIO DE LA CUAL SE REGULA EL USO DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO (SPAM) Y SE DICTAN OTRAS DISPOSICIONES". El Proyecto pretendía regular *“el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por vía electrónica, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.”* Determinaba procedimientos judiciales, y medidas administrativas a cargo de la Superintendencia de Industria y Comercio para sancionar a los infractores de la Ley. Es necesario aclarar el significado del Spam desde el punto de vista del mercadeo, según el cual existen varias técnicas de mercadeo que utilizan la herramienta del CORREO ELECTRÓNICO, como mecanismo para cometer sus fines, estas son: Marketing directo y Marketing por Email. El Marketing directo se define como *“Un sistema interactivo, que utiliza uno o más medios publicitarios para obtener una respuesta medible o una transacción en un determinado lugar”*.

Y el Marketing por E-mail, es el uso del email, en las comunicaciones del marketing, dirigido a un cliente, o para adquirir nuevos clientes, para intentar persuadir a clientes existentes para que realicen una nueva compra, envío de emails, diseñados para alentar la lealtad del cliente y mejorar la relación comercial.

Es una técnica barata y rentable, sus costos son irrisorios, lo cual es de fácil acceso para cualquiera, lo cual permite invadir las bandejas de entrada de miles de correos electrónicos de consumidores potenciales. No existirá gasto de papelería, solo un Ordenador, con acceso a internet, un Programa sencillo y un correo.

Posterior a la expedición de la Ley 1273 de 2009, se da la creación del Ministerio de las Tecnologías de la Información y las Comunicaciones (Tic's) por medio de la Ley 1341 de 2009, en la cual, *“se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”*, quedando en evidencia que para el ámbito nacional colombiano, la información y el dato ameritan ser protegidos en la misma categoría que la vida, honra y bienes de los ciudadanos, ratificándose en la intervención que viene realizando el Estado en aspectos como las actividades de inteligencia y contrainteligencia, inicialmente consagradas en la Ley 1288 de 2009, declarada inexecutable según sentencia C-913 de 2010 de la Corte Constitucional, por vicios de forma y no de fondo; por lo cual, corregidos los mismos, está haciendo tránsito en las cámaras legislativas para su aprobación, por iniciativa del Ministerio de Defensa, donde el eje central de los contenidos, tanto de la ley inexecutable como del proyecto, son el manejo y protección de los derechos fundamentales versus la seguridad ciudadana en el marco de la protección nacional y universal de los mismos. Estamos seguros este proyecto será aprobado

porque no difiere sustancialmente de los propósitos de proteger a los ciudadanos y al Estado armoniosamente en el marco del Derecho Internacional Humanitario.

También vemos esa intervención estatal en la expedición de leyes como la de Seguridad Ciudadana, Ley 1453 de 2011, en la que gran parte de su articulado se encuentra dirigido al uso de las tecnologías de la información y comunicaciones a favor de Estado en la persecución y procedimientos penales, modificando y regulando aspectos como los archivos nacionales de órdenes de captura, permisos relacionados con el porte de armas de fuego, los delitos de utilización ilícita de redes de comunicaciones, transmisión de datos, vigilancia y seguimiento de personas, ordenes de captura, la flagrancia en los casos de grabaciones de video, protección de la imagen de testigos, los medios electrónicos y digitales como medios de prueba, entre otros temas.

Ahora bien; también el poder ejecutivo se ha manifestado en la importancia de la intervención estatal en el uso de las tecnologías de la información y las comunicaciones para evitar la comisión de ilícitos; es por esta razón que expide el Decreto 1630 del año 2011 *“Por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles”* cuyo objeto se encuentra definido en el artículo 1°, así: *“Artículo 1o. OBJETO. El presente decreto tiene por objeto establecer un marco reglamentario que permita restringir la utilización de Equipos Terminales Móviles que han sido reportados como hurtados y/o extraviados en la prestación de servicios de telecomunicaciones móviles, y generar obligaciones a los proveedores de redes y servicios de telecomunicaciones móviles (PRSTM) y a los usuarios, que les permitan tanto a los PRSTM como a las autoridades competentes, hacer uso de la información asociada al número de identificación (IMEI) de dichos equipos terminales para lograr este objeto.*

Se exceptúan del ámbito de aplicación de este decreto, los Equipos Terminales Móviles que se encuentren realizando Roaming Internacional (ó Itinerancia Internacional) en alguna de las redes de los proveedores de redes y servicios de telecomunicaciones móviles que operan en el país.”

Otro importante avance legislativo con relación a los medios informáticos, electrónicos y de telecomunicaciones, es el proyecto de ley N° 241 de 2011 Senado, acumulado con el Proyecto de Ley n° 229 de 2011 Senado “Por medio de la cual se regula la responsabilidad al derecho de autor y derechos de propiedad intelectual en internet”, conocido como Proyecto de “Ley Lleras” que busca, no sólo evitar la violación a los derechos de autor que sucede a gran escala a través de internet, sino también regular la responsabilidad de los proveedores de los servicios de internet frente a la información transmitida.

Desde el punto de vista jurisprudencial y forense se ha dado claridad legislativa y de los jueces al manejo de los sistemas informáticos, haciéndose una clara interpretación de lo que constituye una revisión de los equipos, conciliando la conceptualización de inspección, registro y allanamiento, cuando se trate del mundo digital, a través de las normas procedimentales del nuevo estatuto (Ley 906 de 2004, artículo 232 y ss), y las sentencias C-336 de 2007 y C-334 de 2010 de la Corte Constitucional, que consagran “La relativa flexibilización que el numeral 2° del artículo 250 de la Constitución introduce respecto de los registros (que pueden recaer sobre archivos digitales o documentos computarizados),” y “En cuanto a los allanamientos, registros, incautaciones e interceptación de comunicaciones, la intervención a los derechos se efectúa, en términos generales, sobre los espacios en los que habita o en donde desarrolla su vida y/ o sobre los bienes que le pertenecen o que tienen en su poder, en los que se proyecta y con los que se comunica. Las demás afectaciones de derechos fundamentales del numeral 3° del art. 250 CP., se han decantado por el legislador como intromisiones en la persona

misma del indiciado o imputado, en su intimidad corporal o, como se dijo en la sentencia C-336 de 2007 y se confirma en ésta, en la privacidad sobre su información reservada, como es el caso de sus datos personales o de su información genética. También se incluye allí, cualquier injerencia sobre los derechos fundamentales de personas distintas al indiciado o imputado (familiares, víctimas, terceros).”

No es posible que ninguno de los espacios ocupados por el ser humano escapen al involucramiento con la tecnología, llegando incluso al ámbito de la monitoria electrónica de presos Ley 1142 de 2007, Decreto 177 de 2008, Decreto 3336 de 2008, Decreto 1316 de 2009, Decreto 4940 de 2009, por cuanto, “Es posible pensar en otras formas alternativas a la privación de la libertad que impliquen menores restricciones a los derechos del condenado y que a su vez signifiquen menores costos de ejecución para el Estado. Nos referimos concretamente a la prisión domiciliaria efectivamente controlada y vigilada, arresto de fin de semana, prisión nocturna, arresto de periodo de vacaciones, trabajos a favor de la comunidad y seguimiento electrónico. Este último consiste en someter al interno a un control que permita su ubicación espacial mediante técnicas electrónicas o similares que no afecten su salud ni su dignidad¹⁶¹”.

Como cierre de toda esa ola digital normativa se ha propuesto el Conpes¹⁶² de la Ciberseguridad, que según el Ministerio de las Tecnologías de la información y las comunicaciones (Tic’s):

¹⁶¹ Solicitud de Estudio de Antecedentes de sobre el Proyecto de Ley Estatutaria N° 03 de 2003 Senado. “por el cual se expide el Código Penitenciario y Carcelario”. Realizada el 25 de agosto de 2003, por la Comisión Primera del Honorable Senado de la República de Colombia a la Oficina de Asistencia Técnica Legislativa –OATL-. Consultada el 7 de mayo de 2011 desde: <http://www.secretariasenado.gov.co/estudios-ARD/008%20Sistema%20Penitenciario%20y%20Carcelario.pdf>

¹⁶² “El Consejo Nacional de Política Económica y Social (Conpes) es un organismo técnico asesor del ejecutivo y la máxima autoridad nacional de planeación en el país, siendo el espacio más importante de discusión para la formulación de las políticas públicas.

“Con la aprobación del Conpes de ciberseguridad y ciberdefensa el país contará con una herramienta que le permitirá prevenir y responder amenazas cibernéticas, protegiendo así su soberanía, gobernabilidad e infraestructura crítica entre otras”, señaló el Ministro TIC, Diego Molano Vega.

Con esta iniciativa el Ministerio TIC, emitirá un documento con las directrices en temas de seguridad de la información basado en estándares internacionales, que deberán implementarse por las entidades del sector público para minimizar el riesgo de amenazas informáticas.

De igual manera el Ministerio TIC promoverá planes de educación formal a través del Ministerio de Educación y el Servicio Nacional de Aprendizaje (SENA), para que el sector privado tenga acceso a capacitación en temas de ciberseguridad y seguridad de la información para que estos organismos apoyen la consolidación de la estrategia nacional de ciberseguridad en diferentes regiones del país.

Para proteger a los ciudadanos de los riesgos informáticos, el gobierno creará tres dependencias:

- 1. El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - ColCERT, encargado de coordinar a escala nacional los aspectos de ciberseguridad.*
- 2. El Comando Conjunto Cibernético de las Fuerzas Militares, que tendrá la responsabilidad de salvaguardar los intereses nacionales en el ciberespacio.*

Para coordinar y orientar a los organismos del gobierno encargados de la dirección económica y social y definir las líneas de política, el Conpes realiza el estudio y aprobación de documentos que son presentados en sus reuniones. Los documentos Conpes, son el instrumento técnico de apoyo y coordinación en la formulación de las políticas. Es el Departamento Nacional de Planeación, DNP, quien tiene la labor de producir y presentar los documentos que se discutirán y aprobarán en el Conpes.” (Extraído el 15 de septiembre de 2011, desde: http://www.dansocial.gov.co/index.php?option=com_content&view=article&id=448:conpes&catid=176:participacion)

3. *El Centro Cibernético Policial, estará a cargo de la prevención, la investigación y apoyará la judicialización de los delitos informáticos. Para ello, contará con un comando de Atención Inmediata Virtual (CAI Virtual) para recibir las denuncias de los ciudadanos.*

La creación de estas dependencias dará confianza a los colombianos que cada vez más adelantan transacciones en la web. Según la Superintendencia Financiera, el monto de las operaciones monetarias adelantadas en el 2010 ascendió los 667,6 billones de pesos.

El Conpes de Ciberseguridad y ciberdefensa contempla la creación de la Comisión Intersectorial, encabezada por el Presidente de la República, el Alto Consejero para la seguridad, los ministros de Tecnologías de la Información y las Comunicaciones y Defensa, los directores del DAS y del Departamento Nacional de Planeación. Esta instancia orientará estratégicamente al CoICERT.”¹⁶³

La utilización de las tecnologías de la información y las comunicaciones en beneficio del cumplimiento de los fines del Estado, se ve reflejada en la creación de leyes como la de Seguridad Ciudadana, Ley 1453 de 2011, regulando aspectos como los archivos nacionales de órdenes de captura, permisos relacionados con el porte de armas de fuego, los delitos de utilización ilícita de redes de comunicaciones, transmisión de datos, vigilancia y seguimiento de personas, órdenes de captura, la flagrancia en los casos de grabaciones de video, protección de la imagen de testigos, los medios electrónicos y digitales como medios de prueba, entre otros temas. Y con la Ley 1142 De 2007, Decreto 177 De 2008, Decreto 3336 De 2008, Decreto 1316 De 2009, Decreto 4940 De 2009, que implementan y regulan la vigilancia

¹⁶³ Extraído el 14 de septiembre de 2011, desde: <http://www.mintic.gov.co/index.php/mn-news/188-20110714conpes>

electrónica de presos como reemplazo a la condena formal en centro de reclusión.

En materia procedimental penal, frente a los temas de recolección de la información contenida en medios digitales y la existencia y validez de la prueba informática, tenemos las sentencias C-336 de 2007 de la Corte Constitucional Colombiana, según la cual, “ (...)Es claro entonces, que la búsqueda selectiva en bases de datos conformadas por instituciones o entidades pública o privadas autorizadas para el tratamiento de datos personales, que contienen información confidencial del indiciado o imputado y que por lo tanto no son de acceso público, involucra afectación al derecho fundamental a la autodeterminación informática, por lo que su práctica sólo puede llevarse a cabo previa autorización del juez de control de garantías, quien para la adopción de la autorización correspondiente tendrá en cuenta la legitimidad de la medida atendiendo a su finalidad, así como los criterios de pertinencia, idoneidad y necesidad de la misma que determinen su proporcionalidad en el caso concreto.

(...)”

Ratificando el desarrollo digital colombiano, el Congreso de la República por intermedio del Parlamentario José Fernando Velasco, ha aprobado en primer debate en la comisión primera constitucional del Senado, el día 21 de septiembre, el Proyecto de acto legislativo N° 05 de 2011 “*Por el cual se constituye el acceso a Internet como derecho fundamental, se modifica el artículo 20 de la Constitución Política y se dictan otras disposiciones*” donde se reforma el artículo 20 de la Constitución Política, con el propósito de reconocer el derecho de Internet como un derecho fundamental, que de ser aprobado quedaría así:

“Artículo 20. *Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la de acceder efectivamente a Internet, y la de fundar medios masivos de comunicación.*

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.”

Parágrafo Transitorio. *El Gobierno Nacional contará con un término de tres (3) meses contados a partir de la fecha de promulgación del presente acto legislativo, para radicar ante el Congreso de la República el proyecto de ley que regule el acceso a la Internet.”*

Proyecto que en su parte motiva esboza los criterios que lo llevan a reconocer y a asumir el *“Informe del Relator Especial sobre la promoción y protección del Derecho a la libertad de opinión y de expresión, Frank La Rue”* del 16 de mayo de 2011 del Consejo de Derechos Humanos de la Organización de las Naciones Unidas, cuyos criterios generales son los siguientes:

“La categoría de derecho fundamental se adquiere cuando un derecho humano cumple una de las siguientes reglas: i) que esté incluido expresamente en la Constitución Política en el Título II, Capítulo primero; ii) que se adquiera por conexidad; iii) que esté consagrado en los tratados y convenios internacionales ratificados por el Estado; y iv) que tenga un carácter inherente a la persona humana y no estén señalados en la Constitución.

(...)

El acceso a internet está inmerso en la Constitución Política en el Título II, Capítulo primero; toda vez que se constituye en la materialización de los artículos: 16 (libre desarrollo de la personalidad), 18 (libertad de

conciencia), 19 (libertad de cultos), 20 (libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación) y 27 (libertades de enseñanza, aprendizaje, investigación y cátedra). (...)

Acceder a Internet es tanto un derecho fundamental por sí mismo, como un derecho que puede ser adquirido por conexidad, en tanto que garantiza derechos fundamentales como la libertad de opinión y de expresión y es "facilitador" de derechos económicos, sociales y culturales (el derecho a la educación y el derecho a participar en la vida cultural y a gozar de los beneficios del progreso científico y sus aplicaciones), así como los derechos civiles y políticos (derecho a la libertad de asociación y de reunión).

La Internet permite a los Estados alcanzar la Meta 8F del Milenio: “Desarrollar asociaciones globales”, al garantizar el acceso de las nuevas tecnologías, la información y las comunicaciones a todos; por lo cual, uno de los principales argumentos de la Asamblea General de las Naciones Unidas¹⁶⁴ para declarar el acceso a Internet como un derecho humano fundamental, fue su consideración como herramienta para promover el crecimiento y el progreso de la sociedad y un derecho universal de fácil acceso para cualquier individuo; además, lo reconoce como un derecho que debe “mantenerse en momentos políticos clave como elecciones, tiempos de intranquilidad social o aniversarios históricos y políticos”¹⁶⁵, esto es, que no puede ser suspendido aun en

¹⁶⁴ FORO DIGITAL en Internet disponible en <http://www.forospyware.es/...> Citado en: Exposición de motivos proyecto de acto legislativo N° 05 de 2011 Senado de la República de Colombia. Consultado el 22 de septiembre de 2011, desde: http://servoaspr.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=03&p_numero=05&p_consec=29602

¹⁶⁵ REVISTA Digital Zona franca. Internet un derecho humano, declara ONU. Revista digital. Junio 12 de 2011. Disponible en <http://www.zonafranca.mx/enlinea/blog/> Citado en: Exposición de motivos proyecto de acto legislativo N° 05 de 2011 Senado de la República de Colombia.

estados de excepción, conforme lo establece el literal b) del artículo 29 de la Convención Americana de Derechos Humanos¹⁶⁶.”

Criterios que como lo hemos afirmado recogen el espíritu de las Naciones Unidas que se puede sintetizar en:

“Este informe analiza las principales tendencias y desafíos para el derecho de toda persona a buscar, recibir y difundir informaciones e ideas de toda índole a través de Internet. El Relator Especial Relatoría destaca la naturaleza única y transformadora de la Internet no sólo para que las personas puedan ejercer su derecho a la libertad de opinión y de expresión, sino también un variedad de otros derechos humanos, y promover el progreso de la sociedad en su conjunto.

(...)

El Relator Especial desea subrayar que el acceso a la Internet tiene dos dimensiones: el acceso a contenidos en línea, sin ninguna restricción, salvo en un algunos casos limitados permitidos bajo la ley internacional de derechos humanos, y la disponibilidad de la infraestructura necesaria y la información de las tecnologías de comunicación, tales como cables, módems, computadoras y software, para acceder a Internet en el primer lugar.”¹⁶⁷

Consultado el 22 de septiembre de 2011, desde: http://servoaspr.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=03&p_numero=05&p_consec=29602

¹⁶⁶ COLOMBIA. Corte Suprema de Justicia, Sala de Casación Penal. M.P. Álvaro Orlando Pérez Pinzón. Proceso No 27418 del 2 de mayo de 2007. Bogotá. Disponible en [www.usergioarboleda.edu.co/derecho.../jurisp_mayo_27418\(02-05-07\)](http://www.usergioarboleda.edu.co/derecho.../jurisp_mayo_27418(02-05-07)) Citado en: Exposición de motivos proyecto de acto legislativo N° 05 de 2011 Senado de la República de Colombia. Consultado el 22 de septiembre de 2011, desde: http://servoaspr.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=03&p_numero=05&p_consec=29602

¹⁶⁷Informe del Relator Especial sobre la promoción y protección del Derecho a la libertad de opinión y de expresión, Frank La Rue” del 16 de mayo de 2011 del Consejo de Derechos Humanos de la Organización de las Naciones Unidas. Consultado el 22 de septiembre de 2011, desde: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Es indiscutible los avances significativos colombianos en los temas digitales que esperamos sirvan de impulso al tema en el contexto mundial.

1.8.5. Ley de los Servicios de la Sociedad de la Información y Comercio Electrónico. Expresión máxima de la protección a la información en España.

En palabras de VILLAR URIBARRI (2003), refiriéndose al tema español, y en cuanto a la Ley de los servicios de la Sociedad de la Información y Comercio electrónico, LSSICE, apreciamos lo siguiente: *“En nuestro país, y como resultado de esta iniciativa estatal, hallamos la Ley de los Servicios de la Sociedad de la Información y Comercio Electrónico. Mediante esta Ley, el Estado español ha pretendido dinamizar el tejido empresarial español y, al mismo tiempo, establecer la necesaria protección de los derechos de los usuarios de manera que estos no pierdan sus derechos a favor de la seguridad internacional”* (LOPEZ ZAMORA, P. 2006:180)¹⁶⁸

Indiscutiblemente, esta ley española, representa una expresión de la forma de regular el ciberespacio en la era de la globalización, recogiendo las experiencias de la comunidad económica europea en dicha materia, análisis que acertadamente realiza LÓPEZ ZAMORA, P. (2006) quien manifiesta en la compilación que Emilio Suñe Llinas hizo en el Tratado de Derecho Informático, Volumen II y que gentil y generosamente ha compartido con nosotros:

¹⁶⁸Villar Uribarri, J. M.: “El régimen jurídico de los prestadores de servicios de la sociedad de la información”, *op. cit.*, p. 392 Citado en: LÓPEZ ZAMORA, P. (2006), en TRATADO DE DERECHO INFORMÁTICO VOLUMEN II. Coordinador SUÑE LLINAS, E. (2006) Madrid: Universidad Complutense de Madrid, p. 180

“Así pues, la humanidad ha entrado en una nueva etapa de su desarrollo, en la que la sociedad de la información se presenta como el máximo exponente de las profundas transformaciones tecnológicas acaecidas en los últimos años. Parece entonces evidente que la configuración y difusión de la información contenida en este caudaloso flujo tiene una repercusión directa sobre el mundo de los derechos, las libertades y los comportamientos de muchas personas, a las que puede generar problemas de indefensión. Concretamente, los problemas jurídicos se manifiestan como los más relevantes, puesto que la adecuación de la reglamentación legal del flujo interno e internacional de información y datos se constituye en un reto esencial al que deben enfrentarse los diversos ordenamientos jurídicos.”¹⁶⁹ (LÓPEZ ZAMORA, P. 2006:180)

La LSSI, aunque desarrollando la normativa comunitaria, presenta un concepto de Servicio de la Sociedad de la Información más extenso que el establecido por aquella. Según la Exposición de Motivos de la LSSI, se recoge un concepto amplio de Servicios de la Sociedad de la Información:

“Engloba, además de la contratación de los bienes y servicios por vía electrónica, el suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red), las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de

¹⁶⁹LÓPEZ ZAMORA, P. (2006), en TRATADO DE DERECHO INFORMÁTICO VOLUMEN II. Coordinador SUÑE LLINAS, E. (2006) Madrid: Universidad Complutense de Madrid, p. 180.

instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios, siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.”

Cualquier actividad que, conforme a lo detallado anteriormente, pueda calificarse de servicio de la sociedad de la información, cae dentro del ámbito de la presente Ley, por lo que cualquier persona que la desarrolle está vinculada al cumplimiento de la normativa. En concreto, la definición de Servicio de la Sociedad de la Información que recoge el Anexo de la Ley es la siguiente:

A los efectos de esta Ley, se entenderá por: a) “Servicios de la sociedad de la información” o “servicios”: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

- 1º. La contratación de bienes o servicios por vía electrónica.*
- 2º. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.*
- 3º. La gestión de compras en la red por grupos de personas.*

4º El envío de comunicaciones comerciales.

5º El suministro de información por vía telemática.

6º. El video bajo demanda, como servicio en que el usuario puede seleccione a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1 º. Los servicios prestados por medio de telefonía vocal, fax o telex.

2º. El intercambio de información por medio de correo electrónico u otro medí de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3º Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/194, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sóbre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio le actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4º. Los servicios de radiodifusión sonora, y

5º. El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

Frente a esta Ley en particular, el Instituto Nacional de Tecnologías de la Comunicación, en conjunto con el Ministerio de Industria, Energía y Turismo de España han realizado un análisis amplio de la legislación objeto de estudio en este aparte de la presente tesis doctoral.

Intenco¹⁷⁰ en su análisis a la Ley de la Sociedad de la Información y el comercio electrónico, de diciembre de 2012, ha establecido unos aspectos principales que nos permiten conocer y utilizar la citada ley, así:

“La LSSI se articula en torno al concepto de servicios de la sociedad de la información como todo aquel servicio que represente una actividad económica para el prestador, siendo éste cualquier persona física o jurídica que ofrezca estos servicios por vía electrónica. Entre estos se incluyen: la contratación de bienes y servicios o el suministro de información por vía electrónica y las actividades de intermediación (provisión acceso a Internet, transmisión de datos, copia temporal de páginas web, alojamiento y servicios de búsqueda).

La prestación de servicios de la sociedad de la información dirigidos a destinatarios en España se realizará bajo el régimen de libre prestación de servicios, es decir, no se requiere autorización previa. Salvo para los prestadores establecidos en Estados no miembros de la Unión Europea (UE) o del Espacio Económico Europeo (EEE) que se atenderán a los acuerdos internacionales aplicables. Además la Ley establece restricciones a la prestación de servicios y un procedimiento de cooperación intracomunitario. Es por esto que el ámbito de aplicación de la Ley depende del lugar en que esté establecido el prestador, siendo de aplicación general para prestadores establecidos, o con un establecimiento permanente, en España y a sus servicios. Si el prestador está establecido en países miembros de la UE o del EEE sólo aplica si los destinatarios de los servicios residen en España y si afecta a determinadas materias (propiedad intelectual, contratación,

¹⁷⁰ Instituto Nacional de Tecnologías de la comunicación de España. Pagina Oficial <http://www.inteco.es> Informe de adecuación de la Ley de a la Ley de servicios de la Sociedad de la información y de comercio electrónico. De diciembre de 2012. Tomado desde: https://www.incibe.es/file/oqQycDyL33mC_bcRKSfbbg el 10 de enero de 2015.

comunicaciones comerciales, etc.), en otro caso se aplican los tratados o convenios internacionales. Si el prestador está establecido fuera de la UE o del EEE y dirigen sus servicios a territorio español aplicará la Ley siempre que no contravenga los acuerdos existentes.”

Ahora, frente a la protección de datos personales, Inteco establece que *esta Ley complementa a la Ley Orgánica de Protección de Datos, LOPD en lo relativo a las comunicaciones comerciales por vía electrónica, incluyendo derechos para personas jurídicas. También regula el envío de «publicidad» por esta vía estableciendo una serie de obligaciones y derechos. Entre esa regulación se encuentra particularmente la prohibición del envío de publicidad (spamming) salvo que el destinatario haya prestado su consentimiento o exista una relación contractual previa y regula las ofertas promocionales engañosas.*

Así mismo, Inteco cuando realiza el análisis en cita hace claras referencias a los contratos electrónicos, que se hacen indispensables manifestar en esta investigación, puesto que del desarrollo y ejecución de un contrato electrónico y virtual se pueden desprender infinidad de situaciones y conductas que eventualmente pueden constituirse en delito y precisamente por forma de comisión en ciberdelito, de esta forma el Instituto nacional de tecnologías de la comunicación en España expuso que: *“En cuanto a los contratos electrónicos establece las obligaciones previas y posteriores a su celebración. Además equipara la validez y eficacia de estos contratos, a los realizados en papel, siendo también admisibles en un juicio. Sin embargo, no todos los contratos se pueden realizar por vía electrónica quedando excluidos los contratos relativos al derecho de familia y sucesiones, y aquellos en los que para su validez sea necesaria, la forma documental pública o la intervención de notarios, registradores de la propiedad u otras autoridades. Precisamente, la actividad pública de notarios, procuradores y registradores de la propiedad y mercantiles queda excluida del ámbito de esta Ley. Los prestadores de*

servicios están obligados, y su incumplimiento es motivo de infracción, a facilitar información y a colaborar con la Administración en su labor de control e inspección. En particular a los proveedores de servicios de intermediación para los que establece deberes de colaboración e información sobre medidas de seguridad. Igualmente se obliga a la Administración a facilitar datos e información a consumidores y prestadores.”

1.9. Conclusiones

El mundo occidental ha sido definido en todas las etapas de la historia por grandes revoluciones, en el siglo XVIII la Revolución Francesa generó los cambios más importantes frente a la visión del hombre en el mundo, a finales del siglo XVIII y principios del siglo XIX la Revolución Industrial cambió drásticamente los medios de producción, generando gigantescos impactos en la economía mundial, y finalmente el siglo XX introdujo la Revolución tecnológica, que rige, como lo define Anthony Giddens, la vigilancia de todos los aspectos de la vida social.

Es dicha incursión en la vida social del hombre lo que impulsa a los Estados a crear controles, procedimientos y métodos que permitan regular el trámite de los ciudadanos con los medios de comunicación y de la información, de forma que todas las actividades que incluyan dichos trámites cuenten con la suficiente regulación legal para que las conductas que los incluyan no salgan del margen de la ley.

Sin embargo nos encontramos con la dificultad de regulación legal frente al concepto territorial de la Ley y la jurisdicción de cada uno de los Estados para la persecución de las conductas relacionadas con la información como bien jurídico tutelado o de los medios de información y comunicaciones como

herramienta para su comisión, es por esta razón que nace nuestra necesidad investigativa de desarrollar la presente tesis doctoral denominada *EL DELITO EN LA CIBERSOCIEDAD Y LA JUSTICIA PENAL*.

2. CIBERDELITOS COMO CONDUCTA DENTRO DE LA SOCIEDAD DE LA INFORMACIÓN

2.1. Introducción

La sociedad del conocimiento es generadora de múltiples y diversas realidades. Su surgimiento obedeció a las transformación inteligente del capitalismo, que aprovechando el gran poder de conocimiento generado por la guerra, el uso de la tecnología y la racionalidad de la ciencia, supo crear un nuevo paradigma, en donde la producción de capital a gran escala, tenía menos asiento en la fuerza de trabajo y más en las ideas. Con ella el ser humano entró en una nueva época, marcando así la ruptura con la tradición moderna. Conocimiento y tecnología se convierten, rápidamente, en el mejor aliado de la producción de riqueza, generador de nuevos relatos en las relaciones entre los hombres. Lo virtual es a histórico precisamente porque rompe con la huella, que supo dejar el hombre que nos precede. Lo virtual es hoy, pero desaparece rápidamente dada la magnitud de la información y la velocidad que le es inherente. Ciencia, tecnología y conocimiento se entrelazan en la contemporaneidad con las prácticas de cultura virtualizadas. La realidad de los seres humanos deja de ser un asunto eminentemente físico vinculado con narraciones históricas. La realidad se transmuta y con ella nuevas prácticas culturales van surgiendo. El ser humano sale de su anonimato al ingresar a un mundo potencial y virtual. Su estadía en el mundo deja de ser regional para convertirse en planetaria. El hombre ya no está solo, a él lo acompañan múltiples miradas. A la vez que sale de su soledad, es controlado y por esto mismo su anonimato se traduce en velocidad. Las autopistas espaciales imprimen un nuevo destino, crean otros modos de relación y propician diferentes maneras de estar. El ser humano vive en la sociedad de la velocidad antes que en la del control.

Entre las características principales de la sociedad del conocimiento, se observa la gran circulación de información, las ventajas que tienen los sujetos de acceder en tiempo real a información y el conocimiento; la facilidad para estar al mismo tiempo en múltiples y diversos lugares, el juego diverso de opciones de saber, así como la singularidad en la relación con lo múltiple. Lo lejano se acerca y lo cercano se aleja, principio impensable en la sociedad industrial, moderna y tradicional. La sociedad del conocimiento apoyada en su mejor aliado propicia nuevas formas de saber y genuinas prácticas de conocimiento. El ser humano de nuestros días puede formarse virtualmente, comprar en la distancia, gozar de servicios, bienes y pactar contratos con el cibermercado. La sociedad del conocimiento genera, en singular, una nueva relación con el saber, el conocimiento, los bienes, los servicios y es productora de nuevos patrones de cultura.

Pero esta nueva realidad humana no es tan segura como la anterior. Si la modernidad fue rica por sus sistemas de control, la de la tecnología y de la información lo es por su velocidad. Los peligros son tan reales como lo fueron en la sociedad de tradición. El hacker y los virus constituyen la física de una nueva modalidad del crimen. El primero busca poner en jaque los juegos en el ciberespacio; los segundos son el relato de lo que podríamos denominar como “patología informática”. El virus y el Hacker son la amenaza del presente y del futuro. En este orden, los intentos por regular, controlar y crear una paz ciberespacial, ha obligado a los sujetos internacionales a adoptar medidas, buscando con ello brindarle seguridad a quienes imprescindiblemente viven en esta realidad denominada virtual.

2.2. Derecho Penal Informático.

MÖHRENSCHLAGER, quien expresa: *“cubre todo tipo de hechos donde las formas de procesamiento de datos son el medio de comisión y/o el objeto de ataque u ofensa y representa las bases para la sospecha de que ha sido cometido un delito”*¹⁷¹, concepto ratificado por el grupo de expertos de la OCDE, citado por el mismo autor cuando al referirse al delito relacionado con los computadores a *“... cualquier comportamiento ilegal, no ético o no autorizado, que involucre el proceso o la transferencia de datos”*¹⁷²

El tema del delito informático ha sido objeto del Derecho Informático; por tanto, bajo este presupuesto teórico se estudian tanto las relaciones contractuales que se originan, producto de los nuevos bienes desarrollados como resultado de la Sociedad del Conocimiento. Así como aquellos comportamientos atentatorios del libre ejercicio de la voluntad en la contratación electrónica,

¹⁷¹ Möhrenschrager, M. E., “Computer crimes and other crimes against information technology in Germany” en “Information Technology crime. National legislation and international initiatives”. Ed. Sieber, U., Köln, Berlín Bonn, Manchen: Heymann, 1994, de SIEBER, U., Pág 197. Este artículo se puede encontrar también en la Revue internacional de Droit penal 1993 no. 1-2.

¹⁷² Trabajo de la OCDE en el informe “computer-related Criminality; Anlisy of legal Policy inn teh OCDE Area”, París 15. 11.84 DSTI/ICCP 84.22 citado por SIEBER, U., en “Informations technologie and Strafrechtreform (...)”, Pág. 14 y en “legal Aspects (...)”, pág. 20; también citado por este autor en “Documentación para una aproximación al delito informático Trad. Joshi Jubert, U., en “delincuencia informática”. Ed PPU, Barcelona, 1992, Pág. 66. También partirían de concepciones amplias del concepto de delito informático, MÜNKER, D., op. Cit. Ant. Pág 21 o BARRIUSO RUÍZ, C., en “Interacciones del Derecho y la informática” Ed. Dyckinson. Madrid 1996 (...), Pág. 245. En parecidos términos, si bien de forma más restrictiva, TIEDEMANN, K, definía a la criminalidad informática como *“...todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por ello penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos”*. En “poder económico y delito” Ariel. Barcelona 1985, Pág. 122. En idénticos términos, véase al mimos autor en “Criminalidad mediante computadoras” en Temas de Derecho Penal económico y ambiental” IDEMSA, Lima, 1999, Pág. 481. En similares términos LAMPE, E. J., “Die Strafrechtliche Behandlung der sog. Computer-kriminalität en GA 1975, Pág. 3. WINKELBAUER, W., sostiene que ésta delincuencia es *“... Una delincuencia general con la particularidad de que se realiza en conexión con sistemas de datos o transferencia de datos”*. En “Computerkriminalität und Strafrecht” en CR 1/1985, Pág. 40. En similares términos ROMEO CASABONA, C. M., afirma que la especificidad de estos delitos la aportan junto al ordenador sus funciones propias más importantes, como serían el procesamiento y la transmisión automatizada de datos. En “poder informático (...)”, Pág. 59.

hace referencia a aquellas conductas que entrarían a tipificar el Delito Informático y que en congruencia con la seguridad jurídica, se hace imposible dar respuesta desde la analogía en materia penal.

El devenir histórico nos muestra como legado, que todo cambio económico y tecnológico genera nuevas formas de pensamiento y de comportamiento; es así, por ejemplo, que para mantener cierto tipo de poder, la humanidad ha generado particulares sistemas de gobierno y con base en éstos, determinados tipos de normas jurídicas para revestir de legalidad algunos comportamientos y garantizar el ejercicio del poder.

2.2.1. Clasificación

Según el tratadista José Cuervo es necesario distinguir el medio y el fin en los delitos informáticos, con la finalidad de encuadrar una acción dolosa dentro de este tipo de delitos; el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y la telemática y, el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero.¹⁷³

A continuación la clasificación de los delitos informáticos, valiéndonos del enfoque sistemático:

I. Según BARRIUSO RUIZ¹⁷⁴ los podemos clasificar en:

¹⁷³ Cuervo, José, "Delitos informáticos: protección penal de la intimidad", AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi, No. 006 – Enero del 1999., <http://www.alfa-redi.org/rdi-articulo.shtml?x=207> página web consultada abril 2007.

¹⁷⁴ BARRIUSO RUIZ, Carlos. 1996. "Interacción del Derecho y la informática", Dykinson: Madrid, págs. 245 a 252.

1. Delitos contra la intimidad (artículos 198.1 y 199)
2. De los robos (artículos 239.3, 239.4, 240.2 y 240.3)
3. De las estafas (artículo 249.2),
4. De las defraudaciones (artículo 257),
5. De los daños (artículo 265.2),
6. Relativo a la protección de la propiedad industrial (artículos 274.1 y 274.3),
7. Relativos al mercado y a los consumidores (artículos 279.1 y 279.3).

De acuerdo con PÉREZ LUÑO¹⁷⁵ se puede hacer la siguiente clasificación:

- a) **Desde el punto de vista subjetivo:** se pone el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuestos de criminalidad
- b) **Desde el punto de vista objetivo:** Considerando los daños económicos perpetrados por las conductas criminalistas sobre los bienes informáticos:

- Los fraudes

Manipulaciones contra los sistemas de procesamiento de datos. Podemos citar:

- Los daños engañosos (Data diddling)
- Los “Caballos de Troya” (Troya Horses)
- La técnica del salami (Salami Technique/Rouchning Down)

- El sabotaje informático

¹⁷⁵ PÉREZ LUÑO, A.E.: «Manual de Derecho e Informática», Barcelona, 1996. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 64.

- Bombas lógicas (Logic Bombs)
- Virus informáticos
- El espionaje informático y el robo o hurto de software:
 - Fuga de datos (Data Leakage)
- El robo de servicios:
 - Hurto del tiempo del ordenador.
 - Apropiación de informaciones residuales (Scavenging)
 - Parasitismo informático (Piggybacking)
 - Suplantación de personalidad (impersonation)
- El acceso no autorizado a servicios informáticos:
 - Las puertas falsas (Trap Doors)
 - La llave maestra (Superzapping)
 - Pinchado de líneas (Wiretapping)

c) Funcionales: La insuficiencia de los planteamientos subjetivos y objetivos han aconsejado primar otros aspectos que puedan resultar más decisivos para delimitar la criminalidad informática.

Atentados contra la fase de entrada (input) o de salida (output) del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.

Para JOVER PADRÓ¹⁷⁶ se entendían comprendidos dentro de los delitos informáticos, con anterior al reciente Código Penal:

¹⁷⁶ JOVER PADRÓ, Josep. 1997. *"El Código Penal de la informática"*, X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Pamplona: Aranzadi Editorial, págs. 349 a 370.

- a) **El fraude informático**, ilícitos patrimoniales que Jurisprudencia y Doctrina han calificado como hurto, apropiación indebida o estafa. La estafa se encuentra en la Sección 1ª del Capítulo VI (de las defraudaciones) del Título XIII, del Libro II. El hurto se encuentra en el Capítulo Y del Título XII, del Libro II.
- b) **Los documentos informáticos y sus falsedades**. Se encuentran regulados en el Capítulo II del Título XVIII (De las falsedades).
- c) **Del sabotaje informático**, tipificado como delito de daños y estragos. El sabotaje informático se tipifica a través de los delitos de daños y otros estragos. Los delitos de daños están regulados en el Capítulo IX del Título XIII. Los delitos de otros estragos están regulados en la Sección 2ª del Capítulo I, del Título XVII, del Libro II.
- d) **Los ataques contra la intimidad de las personas**. Encuentran su cauce penal en relación a la informática en el descubrimiento y revelación de secretos del Capítulo Y del Título X (delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio). Este apartado será el objeto del presente trabajo.
- e) **Las defraudaciones a la propiedad intelectual**. Tienen su vía penal en la Sección 1ª del Capítulo XI del Título XIII (delitos contra el patrimonio y el orden socioeconómico).
- f) **Las faltas informáticas**. En el título III (faltas contra el patrimonio) del Libro III en relación a la falta informática.

Para BAÓN RAMÍREZ¹⁷⁷ dentro de la criminalidad informática se distinguen dos grandes grupos de delitos:

Un primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así distinguiremos los delitos:

- Relativos a la destrucción o sustracción de programas o de material,
- Relativos a la alteración, destrucción o reproducción de datos almacenados,
- Los que se refieren a la utilización indebida de ordenadores,

En un segundo grupo se encuadraría la comisión de los delitos más tradicionales como los delitos contra:

- La intimidad,
- La propiedad,
- La propiedad industrial o intelectual,
- La fe pública,
- El buen funcionamiento de la Administración,
- La seguridad exterior e interior del Estado.

ROMEO CASABONA¹⁷⁸, analiza las distintas facetas de lo que llama “las repercusiones de las Nuevas Tecnologías de la Información en el Derecho Penal”, y de esta forma, divide su análisis, en diferentes apartados bajo los títulos de:

¹⁷⁷ BAÓN RAMÍREZ, Rogelio. *"Visión general de la informática en el nuevo Código Penal"*, 1996. en *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, Madrid: Escuela Judicial/Consejo General del Poder Judicial, págs. 77 a 100.

¹⁷⁸ ROMEO CASABONA, Carlos María. *"Delitos informáticos de carácter patrimonial"*, *Informática y Derecho* nº 9,10 y 11. Mérida: UNED, Centro Regional de Extremadura, págs. 413 a 442

- La protección penal de la intimidad e informática,
- La informática como factor criminógeno en el tráfico económico,
- El fraude informático,
- Implicaciones penales de las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética,
- Agresiones a los sistemas o elementos informáticos.

CORREA, siguiendo a UHLRICH, clasifica los delitos informáticos de la siguiente manera:

- a) fraude por manipulaciones de un ordenador contra un sistema de procesamiento de datos,
- b) espionaje informático y robo de software,
- c) sabotaje informático,
- d) robo de servicios,
- e) acceso no autorizado a sistemas de procesamiento de datos,
- f) ofensas tradicionales en los negocios asistidos por ordenador.

TELLEZ VALDÉS¹⁷⁹ clasifica estas acciones en atención a dos criterios:

1. Como instrumento o medios, categoría en la que encuadra a las conductas que él llama “criminógenas que se valen de los ordenadores como método, medio o símbolo en la comisión del ilícito”,
2. Como fin u objetivo, encuadrando en esta categoría a las “conductas criminógenas que van dirigidas en contra del ordenador, accesorios o programas como entidad física”.

¹⁷⁹ **TELLEZ VALDÉS, Julio. 1996.** *“Los Delitos informáticos. Situación en México”*, Informática y Derecho nº 9, 10 y 11, Mérida: UNED, Centro Regional de Extremadura, págs. 461 474.

SIEBER hace una clasificación que responde, no sólo, a un criterio sistematizador vinculado al carácter automático de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conducta. Las conductas más significativas desde esta perspectiva podrían agruparse en estas cinco modalidades principales:

- a) manipulaciones de datos y/o programas, o “fraude informático”,
- b) copia ilegal de programas,
- c) obtención y utilización ilícita de datos, o “espionaje informático”,
- d) destrucción o inutilización de datos y/o programas, o “daños o sabotaje informático” y
- e) agresiones en el hardware o soporte material informático, principalmente “hurto de tiempo del ordenador”.

Por último, siguiendo a DAVARA RODRÍGUEZ¹⁸⁰ dentro de un apartado en el que incluye “La informática como instrumento en la comisión de un delito”, distingue dentro de la manipulación, mediante la informática, dos vertientes diferentes:

- a) Acceso y manipulación de datos y
- b) Manipulación de los programas.

Atendiendo a ello, considera que determinadas acciones que se podrían encuadrar dentro de lo que se ha llamado el delito informático, y que para su estudio, las clasifica, de acuerdo con el fin que persiguen, en seis apartados:

1. Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos,

¹⁸⁰ DAVARA RODRÍGUEZ, Miguel Ángel. 1997 *"Manual de Derecho Informático"*, Pamplona: Editorial Aranzadi, págs. 285 a 326.

2. Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello,
3. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas,
4. Utilización del ordenador y/o los programas de otras persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro,
5. Utilización del ordenador con fines fraudulentos y
6. Agresión a la “privacidad” mediante la utilización y procesamiento de datos personales con fin distinto al autorizado, que será objeto de éste trabajo.

El mismo autor hace otra clasificación siguiendo el orden sistemático del Código Penal en:

- a) Delitos contra la intimidad y el derecho a la propia imagen (arts. 197 a 201).
- b) Delitos contra el patrimonio y contra el orden socioeconómico.
 - b.1.) De los hurtos (arts. 234 a 236) y de los robos (arts. 237 a 242).
 - b.2.) De las defraudaciones.
 - b.2.1.) De las estafas (arts. 248 a 251).
 - b.2.2.) De la apropiación indebida (arts. 252 a 254).
 - b.3.) De los daños (arts. 263 a 267).
 - b.4.) De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.
 - b.4.1.) De los delitos relativos a la propiedad intelectual (arts. 270 a 272).
 - b.4.2.) De los delitos relativos a la propiedad industrial (arts. 273 a 277).
 - b.4.3.) De los delitos relativos al mercado y a los consumidores (arts. 278 a 286).

c) De las falsedades documentales (arts. 390 a 399).

d) Otras referencias indirectas.¹⁸¹

2.3. Definición de Derecho Penal de la Empresa

El tratadista Peruano, Luis Miguel Reyna Alfaro, en su obra del año 2002, profundiza frente a lo que se ha conocido como el derecho penal empresarial, aquellas conductas jurídicas realizadas dentro de las actuaciones de las sociedades comerciales, en las que la dificultad de adecuarlas de forma típica, antijurídica y culpable se hace aun mayor debido a la imposibilidad de declarar responsables a personas jurídica, para iniciar este análisis, Reyna Alfaro¹⁸² empieza por definir empresa, así: *“En nuestro intento por determinar los límites entre el Derecho Penal económico y el empresarial y, consecuentemente, definir lo que éste último es, resulta imperativo determinar previamente el concepto de empresa, aunque no desde una perspectiva mercantil¹⁸³, sino más bien de carácter económico, como la que formula Sánchez Calero, para quien empresa es “organización de capital y de trabajo destinada a la producción o a la mediación de bienes y servicios para el mercado”¹⁸⁴.”*(REYNA ALFARO, L. M., 2002:93)

¹⁸¹ Cuervo, José, “Delitos informáticos: protección penal de la intimidad”, **AR: Revista de Derecho Informático**, ISSN 1681-5726, Edita: Alfa-Redi, No. 006 – Enero del 1999., <http://www.alfa-redi.org/rdi-articulo.shtml?x=207> página web consultada abril 2007.

¹⁸² REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

¹⁸³ Lo que nos llevaría a *afirmar*, erróneamente, que el Derecho Penal de la Empresa regula la responsabilidad penal de las empresas, entendiendo a la empresa en sentido mercantil, como colectividad de personas. En este sentido: Terradillos Basoco, Juan. art. cit., pág. 52. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

¹⁸⁴ Citado por: Terradillos Basoco, Juan. art. cit., pág. 53. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

Ahora, contando con el anterior concepto de *Empresa*, siguiendo el análisis elaborado por Reyna Alfaro, se hace indispensable plantear el concepto presentado por Schünemann, para este autor, *“la criminalidad de empresa es aquella en la que “por medio de una actuación para una empresa se lesionan los intereses externos, incluidos los bienes jurídicos e intereses propios de los colaboradores de la empresa”*¹⁸⁵. No obstante es importante citar a Terradillos¹⁸⁶ cuando dice que *“la definición formulada por el jurista alemán resulta válida siempre que se entienda a la empresa en términos estrictos, caso contrario, un simple caso de violación de la libertad sexual, valiéndose de la jerarquía que a nivel de empresa ostenta el sujeto activo del delito, podría encajar en los términos de la definición de Schünemann”*.

Sin embargo, Terradillos, dentro de su propia definición, se encarga de excluir los delitos informáticos de su concepto de criminalidad de empresa, lo que nos obliga a tener en cuenta su interpretación del concepto de Schünemann, pero alejarnos de su propia definición de criminalidad empresarial y es así que sustentamos nuestra cercanía con el concepto del tratadista peruano Reyna Alfaro, es así como Terradillos, *excluye de su ámbito a las manipulaciones informáticas*, entendiendo que estas *“pueden ser un instrumento de la actividad económica”* y que *“son sólo un medio comisivo susceptible de utilización al margen de la estructura empresarial, al que ha de hacerse frente con tipos genéricos”*¹⁸⁷ (REYNA, L.M., 2002:93), mientras que para Reyna Alfaro, *la información (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos) resulta ser, hoy en día, un valor*

¹⁸⁵ Schünemann, Bernd. Cuestiones Básicas de Dogmática Jurídico-Penal y de Política Criminal acerca de la Criminalidad de Empresa, en: ADPCP, pág. 531-1988. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

¹⁸⁶ *ibid.*, pág. 53 y 54. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

¹⁸⁷ *Ibid.*, pág. 54. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

*económico de empresa perfectamente asimilable dentro del radio de acción del Derecho Penal de la Empresa*¹⁸⁸. (REYNA, L.M., 2002:93).

Tal como hemos argumentado hasta el momento, este medio de comunicación modificó la conciencia, tanto de la práctica empresarial como de la conducta de los particulares, en cuanto al rompimiento de la manera tradicional de ejercer la cotidianidad, lo cual generó nuevas esferas de intercambio socio-cultural; al tiempo que transformó la manera de hacer negocios o administrar las empresas.

La discusión sobre la necesidad de reglamentar la internet se hace evidente en primera medida, dado que son los mismos empresarios los que entienden que si no hay confianza para que los consumidores accedan a esta nueva forma de transacciones mercantiles, será muy difícil que puedan servirse de las bondades que ofrece el uso de las TIC; se precisa una revolución cultural que de hecho ya opera, y en gran medida comienza a posicionarse; no obstante, aún falta mucho camino por recorrer.

De otro lado, tenemos que las mismas asociaciones de consumidores, para los cuales resultan imprescindibles unas reglas claras para depositar su confianza, se han encargado de generar estrategias que les permitan asegurarse en cuestiones como la responsabilidad del oferente, reclamaciones o la protección de su derecho a la privacidad, entre otras, las cuales son ejemplos de una gran variedad de situaciones que comienzan a aparecer en la medida en que las prácticas diarias lo exigen.

¹⁸⁸ Véase mis argumentaciones en: Reyna Alfaro, Luis Miguel. Fundamentos para la Protección Penal de la Información (Almacenada, Tratada y Transmitida mediante los Sistemas de Procesamiento de Datos) como Valor Económico de Empresa, en: REDI, n° 9, Abril 1999. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 93.

En ese sentido, el contexto internacional está dividido en dos grandes paradigmas: de un lado la posición asumida por los Estados Unidos para quienes más que regulación estatal, su posición pretende una *autorregulación*, lo que, en pocas palabras, hace referencia a la autonomía de la voluntad de los participantes en la internet, asociaciones o entidades representativas de los empresarios, las cuales, en palabras de Alonso Ortega Jimenez, “*facilitan el control de los contenidos, con instrumentos como líneas directas de queja del público, para denunciar contenidos considerados inadmisibles.*”¹⁸⁹

Los mecanismos de *autorregulación* son también conocidos como *sistemas de autodisciplina empresarial*, que permitan brindar soluciones globales a problemas globales, generados entre consumidores y oferentes en la red, sin importar el lugar de residencia de ninguna de las partes, a bajo costo, eficaces y de un acceso rápido que permiten respuestas rápidas, sin tener que acudir a los sistemas legales que, por lo general, pueden presentar demoras en la resolución del litigio, carentes de aceptación en la versátil dinámica virtual.

Hacen parte de esta *autorregulación* mecanismos como los Códigos de Conducta, los ADR`s (Alternative Dispute Resolution Systems) y los Iconos de Confianza.

¹⁸⁹ Ortega Jiménez, Alonso, “La regulación de internet”, Revista electrónica alfa-Redi, No. 061, agosto 2003, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9464>, ISSN, 1681-5726, página consultada marzo de 2007.

Estos *sistemas de autorregulación* obedecen a la línea de pensamiento que busca generar una *International Cyber Law* como normativa material diseñada para Internet. “Esta normativa podría adoptar diferentes formas: Códigos de Conducta de los internautas, Autorregulaciones de los Proveedores de acceso a Internet, Usos seguidos en Internet, Principios básicos del *e-business* adoptados por asociaciones profesionales u Organizaciones Internacionales, etc.”¹⁹⁰

El segundo paradigma, liderado por la UE sobre la *regulación a cargo del ente estatal o de iniciativa regional*¹⁹¹, o a través de acuerdos multilaterales, en los que converja la voluntad política de todos los Estados, como el lenguaje de unificación universal, nos coloca de cara a una exhortación al *Derecho Internacional Público*, como herramienta confiable llamada a garantizar los derechos de los usuarios de la red.

Es decir, “*regular los conflictos legales que plantea Internet mediante las tradicionales reglas estatales de competencia judicial internacional que señalan los tribunales estatales competentes para conocer de supuestos internacionales, las clásicas normas de conflicto que fijan la Ley estatal aplicable a las situaciones privadas internacionales, y las conocidas reglas sobre efectos de decisiones extranjeras, que determinan la posibilidad de que decisiones públicas emanadas por autoridades de un país sean efectivas en otros países*”¹⁹².

¹⁹⁰ Ortega Jiménez, Alonso, “La regulación de internet”, Revista electrónica alfa-Redi, No. 061, agosto 2003, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9464>, ISSN, 1681-5726, página consultada marzo de 2007.

¹⁹¹ Vale la pena aclarar que esta tendencia no excluye la posibilidad de que se generen sistemas de autorregulación, un claro ejemplo de ello es la LSSI, en la cual su potencia el uso de los mismos, lo que ocurre es que no desconoce el derecho tradicional.

¹⁹² Ortega Jiménez, Alonso, *La regulación de internet*, Op. Cit. Ortega Jiménez, Alonso, “La regulación de internet”, Revista electrónica alfa-Redi, No. 061, agosto 2003, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9464>, ISSN, 1681-5726, página consultada marzo de 2007.

Actualmente, existen varias experiencias; inicialmente la Convención Europea de 1981 de la cual vale la pena mencionar tres aspectos principales: primero, la creación de un organismo independiente rector de la política de manipulación de datos de carácter personal con el objetivo de proteger el derecho a la intimidad; segundo, la inclusión por primera vez de los principios rectores a que debe ser sujeta la operatoria de un banco de datos de carácter personal, legalidad en el acceso a la información, derecho de acceso, acciones orientadas a la actualización y rectificación de la información personal incorrecta, imposibilidad de la utilización de esa información para un objetivo diferente, declarado en el momento de incorporar esa información en el banco de datos. Por último, la cuestión vinculada al establecimiento de sanciones penales específicas para aquel gestor de un banco de datos personales que viole los principios establecidos en la norma¹⁹³.

Por otro lado, encontramos la legislación a la cual ya hemos hecho referencia, por ejemplo: el *Convenio sobre Cybercrimen*, la Directiva 2003/31/CE, relativa a regular determinados aspectos de los servicios de la Sociedad de la Información, y para terminar la ILSSI, la cual opera como marco jurídico para poner fin a la incertidumbre de los usuarios de la Internet.

A pesar de que la LSSI es un intento de regulación jurídica, no soslaya la posibilidad de que se utilicen mecanismos de autorregulación, como herramientas alternativas; por el contrario, propulsa su empleo, desde luego, bajo unos parámetros claros y sin excluir la intervención de la jurisdicción ordinaria como garantía última.

¹⁹³ Cfr. Clases del Postgrado en Contratación Electrónica, Unidad 5, Universidad de Buenos Aires, 2007.

Así mismo, la Decisión Marco 2005/222/JAI del Consejo de la UE de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información, son intentos por regular la utilización indebida de las TIC.

2.3.1. Posición de las empresas transnacionales del sector financiero, de telecomunicaciones y del software

McAfee

El problema del fraude internacional ha sido planteado por diversos sectores de la sociedad internacional, desde organizaciones internacionales hasta empresas transnacionales; por ejemplo, en un informe presentado por McAfee, sustentado en información del FBI y la inteligencia europea en diciembre de 2006 publicitado en apartes por la Asociación de Internautas¹⁹⁴, se señala que una de las causas del auge del cibercrimen en Europa del este, es el alto grado de desempleo y de los bajos salarios, "muchos de esos cibercriminales ven internet como una oportunidad de empleo", dijo McAfee citando al experto en seguridad en internet del FBI, Dave Thomas."

No obstante, bien sabemos que el problema del cibercrimen se caracteriza por la complejidad que entraña su dimensión, dada la heterogeneidad de factores que convergen en la materialización de cierto tipo de conductas; por tanto, un aporte a enfrentar este flagelo, precisa de la revisión de varios frentes; por tanto, no es exclusivamente el normativo, y de hecho, las grandes empresas mundiales de Internet, por la vía del autocontrol, invierten grandes

¹⁹⁴ *Mafias de internet contratan estudiantes para el cibercrimen*, <http://seguridad.internautas.org/crimeware/txt/984.html>, Informe enviado por Comisión de Seguridad el 09-12-2006, página web consultada, enero 20 de 2007.

cantidades de dinero en investigación y desarrollo, para por la vía de desarrollos tecnológicos, crear mecanismos de seguridad informática, pensando en una mejor atención de los usuarios en este sentido, que de no ser así, no existirían los desarrollos que se han presentado en esta materia.

En el mismo sentido y con la finalidad de identificar los riesgos generados por el cibercrimen y establecer datos cuantificables, el Instituto de Seguridad de Computadoras (CSI) de los Estados Unidos, realiza anualmente un estudio sobre seguridad informática y los crímenes que se cometen con el empleo de computadores, apoyado por la división de delitos informáticos del FBI, con la finalidad de levantar el conocimiento de la seguridad informática y, en consecuencia, ayudar a determinar el alcance de este tipo de delitos en Estados Unidos.

En uno de sus últimos informes para el cual se tomaron como muestra 273 instituciones, entre ellas Corporaciones y Agencias del Gobierno, se evidenciaron alarmantes cifras de aumento del número de casos reportados por violaciones a la seguridad.

Business Software Alliance (BSA)

Otro desarrollo importante desde el sector privado ha sido el abanderado por la *Business Software Alliance* (BSA), la cual es la principal organización dedicada a promover la seguridad y legalidad del mundo digital. Esta organización fue fundada en 1988 y tiene cobertura en 80 países. “La BSA es la voz de los sectores de software, hardware e Internet ante los gobiernos y

los consumidores de todo el mundo. Los miembros de BSA representan a las industrias de mayor crecimiento del mercado internacional”¹⁹⁵.

Entre sus funciones principales está la de brindar “formación a los usuarios de informática sobre los derechos de autor del software y sobre la seguridad cibernética; apoyar las iniciativas públicas que fomentan la innovación e incrementan las oportunidades de negocio y lucha contra la piratería del software”¹⁹⁶.

Según un informe de la BSA, colgado en el 2007 “el índice de piratería de programas informáticos, en 2001 fue del 40%. Desde 1994, este índice ha disminuido considerablemente y las razones que han llevado a esta disminución han sido, entre otras:

- Las compañías de software han luchado por mantener el desarrollo del mercado mundial del PC y tienen presencia de ventas legales en todo el mundo, facilitando por tanto, la compra legal del software.
- Las empresas de software tienen disponibilidad de un servicio de soporte, que constituye una razón importante a la hora de comprar una copia legal de un programa.
- BSA y SIIA han realizado campañas de información acerca de la necesidad de comprar versiones legales de software, haciendo hincapié en los derechos de la propiedad intelectual, al mismo tiempo que se han desarrollado acciones legales para evitar este tipo de delito.
- Las empresas se han concientizado del riesgo que supone, para su imagen y credibilidad, la utilización del software ilegal.

¹⁹⁵ BSA, *Acerca de BSA*, <http://www.astrolabio.net/canal/contenido/la-pirateria-informatica-1013677.php>, página web consultada en enero de 2008.

¹⁹⁶ *Ibíd.*

- Ha aumentado la colaboración por parte de los gobiernos, a la hora de ofrecer protección legal a la propiedad intelectual y penalizar la piratería¹⁹⁷.

La BSA considera que lograr una red segura es todo un proceso; inicialmente requiere de la aprobación de políticas de seguridad fuertes, un despliegue a través de los medios de comunicación que demuestren la seguridad del software, así como aplicaciones como antivirus, cortafuegos, la detección de intrusión, la encriptación, la infraestructura de clave pública (PKI) y la dirección de vulnerabilidad, y, para las grandes organizaciones, la existencia de políticas de entrenamiento para profesionales en seguridad¹⁹⁸.

Microsoft

Otra empresa que ha tomado una posición importante frente al sabotaje informático es la Microsoft, incluso hasta ofrecer cuantiosas recompensas para capturar a creadores de virus; éste fue el caso de la recompensa ofrecida para la captura de los creadores de los virus del MS Blast y Sobig, los cuales en el 2003 fueron los responsables de cuantiosas pérdidas económicas; con esta decisión la Microsoft, fue la primera compañía privada en ofrecer recompensas por la identificación y denuncia de cibercriminales¹⁹⁹; su apoyo

¹⁹⁷ BSA, "Información sobre lucha contra la piratería", <http://bloc.pragma.cat/la-bsa/> página web consultada en enero de 2008.

¹⁹⁸ Cfr. BSA, "Security and Cybercrime", <http://www.delitosinformaticos.com/03/2007/propiedad-intelectual/segun-la-bsa-el-robo-de-informacion-y-descarga-de-software-ilegal-son-los-mayores-peligros-en-internet> página web consultada en enero de 2008.

¹⁹⁹ BBC Mundo/Economía, Microsoft contra el "cibercrimen", miércoles, 5 de noviembre de 2003, http://news.bbc.co.uk/hi/spanish/business/newsid_3245000/3245243.stm, página visitada en abril de 2007.

es contundente para ayudar al FBI y a la INTERPOL, con la finalidad de capturar piratas cibernéticos.

Además del compromiso asumido con las autoridades policiales, cuenta con un portal en la red destinado a ofrecer herramientas cognoscitivas para contrarrestar al cibercrimen y participar en los debates académicos propuestos por las universidades; ejemplo de ello es el *Taller de capacitación para manejo y seguimiento de incidentes en Internet*, realizado en países como Venezuela y Colombia a finales del 2007, a cargo de Marlon Fetzner, quien es el comisionado del tema para el área de Latinoamérica, que acompañado de Andrés González se han convertido en unos verdaderos profetas del tema para el mundo.

Vale la pena señalar que el evento realizado en Colombia, en la Universidad Externado, se logró en razón a la invitación cursada dentro del Plan Estratégico de la Línea de investigación Derecho y Nuevas Tecnologías de la Universidad Santiago de Cali, marco en el cual se realiza esta investigación.

Con este tipo de eventos preventivos, la Microsoft pretende educar a los cibernautas, quienes son, en últimas, los que por desconocimiento, generan el riesgo de contaminación de sus equipos y propagan diversos tipos de virus, que pueden incidir en la expansión de amenazas al sistema informático en general.

En este sentido, Jackeline Marcuchi pareciera justificar las medidas preventivas de la Microsoft al explicar que “*el Internet es “inherentemente*

inseguro” y generalmente la persona que hace uso del Internet está insegura acerca de los riesgos, toda vez que la mayoría de la información que se maneja por Internet es de recuperación. Las transacciones, a saber, por Internet son realizadas a través de una red pública que está abierta y disponible, incluyendo criminales”²⁰⁰. Por tanto, una de las principales estrategias que deben implementarse para enfrentar el sabotaje informático, se relaciona directamente con la capacitación de los cibernautas, siendo imprescindible, el autocontrol como cultura, convirtiéndose en la mayor herramienta de prevención en este sentido.

2.3.2. Características de la Criminalidad Empresarial

Dentro de los principales elementos que caracterizan a la Criminalidad Empresarial, Zúñiga Rodríguez, Laura las ha identificado claramente y han sido reproducidas por REYNA ALFARO, L. M. (2002:95) así:

Multiplicidad de sujetos activos.- Al ser las empresas entes de carácter colectivos, sus actividades se desarrollan mediante la participación de múltiples sujetos que actúan para proteger los intereses del ente colectivo, lo que genera dificultades en la determinación de responsabilidad penal sobre todo en empresas con complejos sistemas de distribución de funciones.

Afectación de Bienes jurídicos Colectivos.- Resulta evidente que los conductas en el seno de las agrupaciones tienden a afectar bienes jurídicos de carácter colectivo o macro social, ligados al propio

²⁰⁰ Marcuchi Jakeline, citada por Sergio Rodríguez Azuero, Referencias a la contratación bancaria electrónica en Colombia, en RINCÓN CÁRDENAS, E. (Eds) 2006. Contratación Electrónica, Bogotá D.C.: Centro Editorial Universidad del Rosario. p. 105.

funcionamiento del sistema social, como son, por ejemplo, el medio ambiente, el mercado de valores, el sistema socio- económico, etc., intereses que resultan vinculados a la propia actividad de la empresa, macro entes que provocan lesiones o puestas en peligro de bienes jurídicos igualmente macros, todo lo cual deriva en la indeterminación de las víctimas afectadas²⁰¹.

Diversidad de Nexos Causales y problemas en la determinación de responsabilidades. - Los procesos de producción, distribución y venta, de bienes y servicios generan una serie de problemas en la determinación de la participación y, en consecuencia, en la atribución de responsabilidad penal, como ocurriera en los casos de la Colza, Lederspray, entre otros²⁰². (REYNA, L.M., 2002. P. 94-95)

2.4. CRIMINALIDAD INFORMÁTICA

Ahora frente al tema de la Criminalidad informática vemos que este tipo de alta tecnología posee unas características especiales dentro del plano jurídico que deben ser analizadas y que CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H. (2009).²⁰³. Han definido así:

²⁰¹ *Zuñiga Rodríguez, Laura. Modelos de Imputación Penal para sancionar la Criminalidad de Empresa en el CP Español de 1995, en: RPCP, n° 7-8, pág. 966-967, Lima, 1999. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 95.*

²⁰² Con mayores referencias: Hassemer, Winfried & Muñoz Conde, Francisco. La Responsabilidad por el Producto en Derecho Penal, Edit. Tirant lo Blanch, Valencia, 1995; Rodríguez Montañes, Teresa. Consideraciones Generales acerca del desarrollo actual de la Teoría del Delito, a propósito del problema de la responsabilidad penal por el producto, en: Debate Penal, n° 14, pág. 81 y ss., Lima, 1997; Romeo Casabona, Carlos María. Límites de los Delitos de Comisión por Omisión, en: Debate Penal, n° 14, pág. 103 y ss., Lima, 1997. Citado en: REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores. P. 95

²⁰³ PEÑA ALONSO, Javier, "Delitos en Internet". Disponible en <http://www.portaldeabogados.com.ar/noticias/derin03.htm>. Citado en: CASTRO ARGÜELLO,

- *En el plano jurídico penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos. Esto que podremos observar y analizar en el transcurso del presente trabajo, nos orienta en la dirección que tanto los delitos contra la propiedad, los delitos contra el honor, los delitos contra el orden público, entre otros, se manifiestan hoy potenciados en razón del aumento constante de acceso a las nuevas tecnologías. Y por otra parte, nuevas situaciones de hecho que afectan bienes no tutelados tradicionalmente por el derecho penal, abarcando las grandes redes de información mundial, como puede ser la web y las comunicaciones electrónicas en combinación de diversos medios informatizados.*
- *La criminalidad informática se caracteriza por las dificultades que entraña descubrir, probar y perseguir los delitos. Tanto las empresas (por su repercusión económica) como así también los Estados de diversos países, se han procurado organizar y establecer mecanismos tendientes a fortalecer los sistemas de seguridad informática, realizando investigaciones proactivas en la búsqueda de vulnerabilidades antes de que fuesen descubiertas por otros. La aplicación casi universal de medidas eficaces de lucha contra el delito será necesaria porque las nuevas tecnologías pueden ser explotadas por delincuentes casi sin ninguna de las restricciones que le imponen a los delincuentes tradicionales las fronteras nacionales. Mientras que los delincuentes tradicionales se ven limitados por factores como la distancia geográfica, los controles aduaneros y la necesidad de tener acceso físico a las víctimas, los delincuentes electrónicos pueden operar remotamente y con una impunidad real desde cualquier jurisdicción que carezca de legislación suficiente o de la voluntad o la capacidad de aplicarla, o a través de varias jurisdicciones. El hecho de que las tecnologías y los delitos que dependen*

de ellas sigan evolucionando requerirá un esfuerzo mundial para seguir los nuevos acontecimientos, elaborar respuestas eficaces y difundirlas con suficiente rapidez para que los organismos encargados de aplicar la ley²⁰⁴ puedan perseguirlos eficientemente, con resultados acordes a los reclamos de la sociedad.

- *La precariedad del sistema jurídico penal que cuenta con una novedosa reforma de la materia, refuerza la tendencia a no denunciar estos delitos, para evitar la alarma social o el desprestigio que podría derivarse de su conocimiento. Esto es sumamente comprensible debido a la gran penetración de las nuevas tecnologías en toda sociedad y de las constantes inversiones que las empresas llevan a cabo en cada uno de sus procesos económicos, incluidas las de seguridad informática. Hoy en día los virus suponen el problema más común, junto con el robo de información confidencial, situaciones que conforman la llamada “cifra negra” de la delincuencia informática²⁰⁵. Además de lo expuesto, la*

²⁰⁴ Naciones Unidas, Consejo Económico y Social, Comisión de Prevención del Delito y Justicia Penal, “Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas”. 10° periodo de sesiones, Viena, 8 a 17 de mayo de 2001. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 82.

²⁰⁵ Encuesta sobre seguridad realizada por el FBI - El Computer Security Institute y el FBI toman el pulso a la seguridad en las nuevas tecnologías de miles de empresas de los Estados Unidos. La encuesta realizada entre casi 500 empresas estadounidenses representativas de todos los sectores, se toma como punto de referencia ante la seguridad informática y las empresas. A lo largo de casi una década cada documento ha sido testigo de un cambio de actitud hacia el problema que supone una Internet cada vez más hostil, y hoy en día revela que la seguridad es una parte prioritaria del presupuesto de toda compañía. Por ello en 2004 vuelve a bajar el índice de ataques exitosos, que viene descendiendo desde 2001. Aun así, el 53% de los encuestados declara haber sufrido un acceso no autorizado a sus sistemas. El cambio más sorprendente se observa en el número de ataques provenientes del exterior e interior de la red corporativa, que si bien el año pasado correspondían al 20 y al 80% respectivamente, este año prácticamente se igualan. Los virus suponen el problema más común, afectando al 78% de los encuestados. De hecho esta lacra es la que más cuesta a las compañías, seguido del robo de información confidencial, abusos desde el interior y las brechas en redes inalámbricas. Del estudio también se desprende que los ataques DoS (denegación de servicio o “denial of service”) siguen siendo de los ataques más perniciosos económicamente para las empresas. Disponible en <http://delitosinformaticos.com/seguridad/noticias/109178894685135.shtml>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 82.

mayoría de los expertos cree que formas comunes de delitos relacionadas con las redes informáticas no son suficientemente denunciadas, porque las víctimas no comprenden que lo han sido, quizá no comprenden que el comportamiento de que se trata es un delito²⁰⁶.

- *La insuficiencia de los instrumentos penales, en el contexto anterior a la sanción de la ley 26.388, para evitar y castigar las distintas formas de criminalidad informática, suponía un reto para la política criminal de los próximos años. Por supuesto, fácil de verificar desde el momento en que hoy podemos encontramos con “paraísos informáticos” donde la delincuencia informática conforma un elemento más de la falta de regulación en materia de las nuevas tecnologías de la información y comunicaciones.*
- *La existencia de redes internacionales como Internet abre la posibilidad de transgresiones a nivel mundial y con un gran potencial de impunidad. Las conductas no se realizan en un solo acto, sino en una serie continuada de ellos.*
- *Los daños pueden ser experimentados en un país distinto a aquel donde se encuentra el delincuente físicamente. Fenómeno que representa un gran problema referido a su perseguibilidad, no tanto su identificación y ulterior tipificación. El reto probatorio es en estos aspectos fundamental, pero lo más importante son las trabas que plantean los límites de la jurisdicción, nacionalidad del autor del hecho y el bien jurídico ofendido. Siendo relevante el origen y destino, no los saltos en las conexiones o utilizaciones mediatas de sistemas de tránsito hacia el fin delictivo²⁰⁷.*

²⁰⁶ Naciones Unidas - Consejo Económico y Social - Comisión de Prevención del Delito y Justicia Penal - “Conclusiones del estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas”, 10° periodo de sesiones, Viena, 8 a 17 de mayo de 2001. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 83.

²⁰⁷ VILA LOZANO, Jorge, “Delito informático y tecno-era”, p. 8. Disponible en www.fiscalia.org. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 83.

- *Una vez realizados, es posible eliminar toda evidencia de su comisión, lo que produce dificultades en el descubrimiento y prueba.*
- *Con frecuencia su ilegalidad no es clara (depende el país donde el delito se verifica), resultando las leyes penales tradicionales como insatisfactorias para la prevención del nuevo fenómeno²⁰⁸, tornando casi imposible su persecución y castigo.*
- *Una característica general de este tipo conductas disvaliosas, es que, en la mayoría de los casos detectados, el accionar del sujeto activo es repetido varias veces en el tiempo. Lo que sucede es que una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de “manipulación del programa”, la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active²⁰⁹.* CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H. (2009:81-84)

Posterior al análisis de las características enunciadas en párrafos anteriores, la conclusión clara del autor en cita y que es compartida por nosotros se encamina a demostrar que más allá de la identificación de las conductas desde la dogmática penal y el reconocimiento criminológico de sus sujetos activos es de vital importancia la política criminal de los Estados dirigida a combatir estos nuevos delitos de forma nacional y trasnacional.

²⁰⁸ FREELAND, Alejandro, “Internet y derecho penal”, J.A.-2000-II-769. Lexis N° 0003/007609. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 83.

²⁰⁹ LORENZO, Patricia, disponible en <http://www.monografias.com/trabajos12/conygen/conygen.shtml>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 84.

2.4.1. Necesidad de una Política Criminal Informática

Dentro del ámbito colombiano tuvimos la fortuna de participar en el desarrollo legal contra los delitos informáticos, así fue como finalmente y, ya en el 2007, la Universidad Santiago de Cali abrió un espacio propositivo de discusión: el Primer Foro Internacional sobre Delito Electrónico. Esta propuesta académica surge como iniciativa jurídico-política que acompaña la presentación de un Proyecto de Ley, que propone la adición del Código Penal vigente con la tipificación de conductas que aún no se encuentran incluidas en este ordenamiento. Dicho foro responde a las investigaciones realizadas en el marco de la Línea de Investigación Derecho y Nuevas Tecnologías, la cual nutre una serie de actividades que buscan aportar al diseño de políticas claras en contexto nacional.

El foro contó con dos ejes temáticos: el Jurídico y la Teleinformática, en el entendido de que no basta con la creación de normas jurídicas ajenas a la realidad; por el contrario, se vinculó la perspectiva tecnológica, el discurso de las ingenierías para, en ese sentido, contar con una visión holística del problema del cybercrimen.

Los temas desarrollados dentro del contexto jurídico respondieron a los contratos de alta tecnología, la firma electrónica, la protección de datos personales y del e-mail, la defensa jurídica, el régimen jurídico de la compra a distancia, la banca por Internet, protección de marcas y dominios en Internet, los contenidos ilícitos en Internet, un estado del arte en las investigaciones

sobre el delito informático, el derecho a la intimidad y, finalmente, la propiedad intelectual.

Para el desarrollo de estos temas, se contó con la participación de especialistas como la abogada Andrea Bonnet; su exposición se centró en presentar un panorama nacional e internacional sobre las sanciones relativas al uso de datos personales en Argentina, Colombia, Ecuador, Estados Unidos y España.

De otro lado, Carlos Álvarez²¹⁰, preocupado por la impunidad frente a los delitos informáticos, planteó el debate sobre las estrategias más efectivas para abordar este fenómeno, la conveniencia de un proyecto nacional o internacional, específicamente el Convenio sobre Cibercriminalidad. Señaló que los Estados precisan del desarrollo de procedimientos y herramientas forenses digitales estandarizadas, lo cual deviene en la uniformización legal. Sostiene que en una época globalizada es absurdo pretender ser una isla, de tal manera que considera que la mejor estrategia debe ser la ratificación de un instrumento internacional, que regule la materia y que permita armonizar las legislaciones de los Estados del Sistema Mundial, puesto que el cybercrimen es transfronterizo; por lo tanto, se necesitan medidas que no se diluyan en la legislación de cada país.

El tema de las entidades de certificación digital, fue abordado por Claudia Milena Botero G²¹¹, que manifestó que las modalidades de los negocios electrónicos exigen de un marco jurídico que permita generar confianza entre los usuarios, ante los riesgos que plantea la Internet, tales como: la suplantación de identidad, la alteración de los mensajes de datos, el rechazo

²¹⁰ Gerente de Asuntos Legales para asuntos Andinos de la Sony.

²¹¹ Abogada Especialista en Derecho de las Telecomunicaciones y del Comercio Electrónico.

o repudio de la información y la pérdida de confidencialidad y, precisamente, las entidades de certificación establecen los términos de confianza que requieren los usuarios para el desarrollo del comercio electrónico, a través de la firma digital, los certificados digitales y las entidades de certificación digital.

Por lo mismo, hace referencia a los instrumentos internacionales existentes, la UNCITRAL²¹², UIT²¹³ así como a las políticas generadas al interior de procesos de integración regionales como la CAN, el MERCOSUR, la ALADI y el ALCA. Finalmente, señaló el contexto nacional.

Paralelamente, Freddy Bautista²¹⁴ presentó una estadística de los delitos informáticos más comunes cometidos por año; en ese sentido, en el 2002 en orden de importancia fueron: el fraude en sitios de compra y venta en línea, pornografía infantil, amenazas, calumnias e injurias y violación a la propiedad intelectual. En el 2003, de igual manera, los fraudes en sitios de compra y venta en línea, las estafas nigerianas²¹⁵ con falsas ofertas de trabajo y otros relacionados con narcotráfico y terrorismo. En el 2004, además de los anteriores, se da inicio al uso de spyware, las transferencias ilícitas de dinero, la vulnerabilidad en servicios de banca On line, la denegación de servicios, el tráfico de bases de datos y los llamados Dialers²¹⁶

²¹² CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) <http://www.uncitral.org/pdf/spanish/texts/payments/guarantees/guarantees-s.pdf>, página consultada Febrero de 2008.

²¹³ Unión Internacional de Telecomunicaciones

²¹⁴ Mayor del Ejército Nacional, miembro Grupo Investigativo Delitos Informáticos de la Dirección de Investigación Criminal, DIJI.

²¹⁵ Esta serie de correos pertenecen a una "corriente" por así llamarla, de estafas llamadas "Nigerianas", porque al principio, cuando salieron a relucir, eran practicadas precisamente por gente de Nigeria, consistían en e-mail que informaban el legado de una herencia, un dinero que por equivocación se le debe al destinatario y debe confirmar sus datos para que le sea reembolsado, entre otros.

²¹⁶ O pago por servicio; hace referencia al servicio que se ofrece para pago por el destinatario y que en ocasiones devienen en estafas.

En el 2005 encontramos conductas como el *phishing*²¹⁷, la revelación de secretos industriales, secuestros de cuentas de correo y suplantación de identidad en el sistema financiero. La tendencia para el 2006 adiciona las conductas anteriores y se presentan *daños y sabotajes en bases de datos*, servicios Web, así como el robo de información.

En la conclusión, la ponencia plantea la ausencia de legislación específica que contenga el tema del Delito Informático, derivado en impunidad, así como la débil cultura de la prueba digital (Policía-Fiscales y Jueces-Particulares), lo cual va de la mano con el desconocimiento del tema por parte de las autoridades judiciales y de policía. La creciente Inseguridad Informática, tanto del sector público como del privado y, la rápida transición y utilización que hacen los delincuentes de medios tecnológicos a través de la red.

Considera necesaria la aplicación de la Colaboración Internacional, así como el establecimiento de protocolos y procedimientos más ágiles de cooperación y la ratificación de la Convención Iberoamericana de Cibercrimen.

En otra de las ponencias presentada, se expuso sobre el Derecho de Revocación, Derecho de arrepentimiento y Derecho de Desistimiento, los cuales, propone, deben ser entendidos como un derecho constitucional por la vía de protección al consumidor.

²¹⁷ “Es una modalidad de estafa diseñada con la finalidad de robar la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.” *Todo lo que debe saber acerca del "phishing"*, en www.microsoft.com/latam/seguridad/hogar/spam/phishing.mspx, página consultada marzo 2007.

Entre las conclusiones que se plantearon, puede decirse que la economía de masas requiere de un tratamiento diferente al del comercio tradicional, para lo cual existen algunos derechos que pueden aplicarse en beneficio de la parte débil del contrato, que en este caso está dado por el consumidor; este derecho es el de revocación, el cual es un derecho fundamental universal que tiene el consumidor de conformidad con el artículo 94 Superior.

Finalmente, el Profesor Doctor Rodolfo Daniel Uicich de la Universidad de Buenos Aires, abordó el problema a través de una propuesta sobre la necesidad de establecer una política frente a los delitos informáticos, para lo cual, inicialmente realizó una revisión de los delitos informáticos, sus características, así como la tipificación internacional desde organizaciones internacionales como la ONU, hasta las legislaciones nacionales; por último esbozó el problema que existe actualmente frente a la conveniencia de establecer una legislación internacional. En cuanto el componente teleinformático hizo referencia a aquellas conductas realizadas por los llamados “piratas informáticos” sobre la realización de conductas ilícitas tales como: Haquers, Crakers, Worms²¹⁸, Spyware²¹⁹, Adware²²⁰, Phishing²²¹, Firewall²²², Programas de Acceso Remoto, Espionaje Industrial y Comercial Teleinformática y el Sistema de Gestión de Seguridad Informática.

En este contexto, se presentó una investigación realizada por el Grupo de Investigación COMBA I+D, adscrito a la Facultad de Ingenierías de la Universidad Santiago de Cali, con el tema “Las Redes Inalámbricas, cambiando la seguridad informática de su hogar”; la ponencia gira en torno a

²¹⁸ Virus o Gusanos

²¹⁹ Programas de Espionaje

²²⁰ Programas recopiladores de Información

²²¹ Programas Duplicadores de Páginas

²²² Hardware y Software para protección de sitios conectados a Internet

la necesidad de promover la protección inalámbrica de los usuarios de Internet, a través del uso de la técnica War-x²²³.

Continuando con el tema de la seguridad informática, Juan Carlos Reyes Muñoz miembro de Seltika²²⁴ abordó las razones por las cuales es necesaria la seguridad de la información, definió las amenazas y ataques más frecuentes, así como su impacto y, finalmente, hizo referencia al tipo de crímenes que se realizan a través de la computadora.

De otro lado, Miguel Villalobos como representante de la Superintendencia Financiera de Colombia, encaminó su disertación hacia las estrategias que deben ser empleadas para brindar seguridad y eficiencia en la prestación de servicios financieros. Consideró que las medidas adoptadas actualmente en el sistema colombiano están encaminadas a proteger al consumidor financiero, con la finalidad de Incrementar la confianza en el sector financiero.

Este evento hace parte del último debate académico realizado actualmente; a través de él, se logra evidenciar la preocupación que, desde la academia, genera el actual limbo jurídico en el que nos encontramos, dado que adolecemos de una legislación clara, nacional e internacional, que permita prevenir y sancionar los daños que pueden generarse a la información.

²²³ Los hackers pueden descifrar y leer datos en conexiones inalámbricas protegidas por encriptación WEP (encriptación inalámbrica del estándar básico 802.11), además pueden tener la capacidad de acceder a datos de la red cableada a través de un punto de acceso Wi-Fi. Análisis de la seguridad de las redes Wi-Fi usando las técnicas War-X. Cfr. REVISTA S&T: SISTEMAS & TELEMÁTICA, 1692-5238, Universidad ICESI.

²²⁴ Seguridad Informática y Tecnología Ltda., es una empresa asesora encargada la prestación de servicios especializados de Seguridad Informática en Colombia.

Este foro en sentido general, arrojó como conclusión que el campo de las ingenierías no espera soluciones de tipo jurídico, ante la masificación y proliferación del cibercrimen; su postura es de auto-seguridad, y desarrolla la tecnología encaminada a la protección de software y sistemas de información. Esperar una respuesta jurídica en un mundo globalizado y dinamizado a través de la red, se constituye en una herramienta aún en construcción y el “cibermundo” no da espera.

A continuación encontramos algunas citas que permiten determinar la importancia de un desarrollo criminológico y de política criminal que genere un amplio campo de injerencia dentro de los delitos informáticos

Porque una buena Política Criminal ha de tomar conciencia de que existen causas sociales que impulsan a delinquir. Romagnosi citaba entre ellas: las necesidades perentorias de subsistencia, la escasa vigilancia, la injusticia, los déficits de educación (Romagnosi (1852) citado por Herrero, 2007: p. 83).

Una política criminal es una toma de posición sobre la tipificación penal. Sobre qué tipificar y qué pena instaurar como sanción, qué tipo de control social, en últimas una reflexión sobre la ley penal su vigencia de cara al tipo de sociedad.

El programa de la Política criminal [consiste en] reglas para la limitación de las penas cortas de privación de libertad, libertad provisional, caución preventiva, penalidad sin prisión, reprensión judicial, transformación de la multa, prolongación de la pena, etcétera (Q. Saldaña (1923) citado por Herrero, 2007: p. 83)

La finalidad de la política criminal es *ser crítica de la legislación penal vigente partiendo de los criterios ofrecidos por los fines de ese Derecho*

y del seguimiento de sus resultados y el de proponer medios específicos para la reforma de aquél, el autor alemán hacía descansar a dicha Política, sirviéndose del método adecuado, en la investigación causal del delito y de su consecuencia, la pena o la medida de seguridad (Q. Saldaña (1923) citado por Herrero, 2007: p 84).

Definición de política criminal

El conjunto sistemático de principios, garantizados por la investigación científica de las causas del delito y de la eficacia penal, conforme a los que el Estado orienta la lucha contra el crimen a través de la pena y otras formas de ejecución similares (Liszt (1889) citado por Saldaña citado por Herrero 2007 p. 85).

Decisiones que pueden tomarse con criterios político criminales hacer desaparecer, al máximo, las penas cortas de prisión y extender, por el contrario, la pena de multa; aplicar la condena condicional siempre que fuera aconsejable y factible; tratamiento profiláctico de la proclividad criminal en desarrollo, haciendo frente a la habitualidad y aprendizaje delictivos. Con este fin, entre otros, habría que prestar especial atención a la forma de ser y de reaccionar del delincuente y a sus motivaciones; tratamiento del estado peligroso en cuanto tal; poner en práctica medidas educativas. Sobre todo, para los jóvenes delincuentes; la admisión de medidas de seguridad para supuestos señalados de anormalidad mental del infractor o para delincuentes en que existiese la probabilidad de corrección o readaptación (Herrero, 2007: p. 85)

La indagación de la ciencia penal requiere de una visión horizontal o integral

De aquí la necesidad (...) de utilizar, también, los conocimientos de la Sociología criminal (Herrero 2007: p. 86).

Disertación que permite fundamentar la reflexión sobre el ciberdelincuente

Lo que aparece técnicamente como delitos no son más que el iceberg de conflictos o disfuncionalidades sociales y políticas; con el sistema penal éstos se reprimen y se reconstruyen (Herrero, 2007: p. 88)

Hacen parte del objeto de estudio de la criminología *los comportamientos socialmente dañosos no incluidos dentro de las clasificaciones legales y frente a los cuales es válido plantear una "nueva etiología" (BARATTA, 1990, 108), frente a éstos la óptica penal no sólo es innecesaria sino contraproducente para las disciplinas que los tratan (Herrero, 2007: p. 88)*

La política criminal es esencial para establecer unos *criterios de enfrentamiento al delito [y tener así] una visión no sólo penal, sino también sociopolítica, del fenómeno de la delincuencia (Herrero 2007: p. 89)*

Complementariedad de la política criminal y el derecho penal

La política criminal es el complemento del sistema penal puesto que *la auténtica Política criminal es la que empieza tratando de evitar disfunciones en el ámbito de la Política general y, desde luego, en el campo de la Política social (en el campo de la educación y de la formación profesional, en la política de empleo, de familia, del tiempo libre juvenil), posteriormente el papel del sistema penal será fundamental para el tratamiento de la delincuencia en acto (Herrero, 2007: p. 89).*

¿Qué elementos requiere una política criminal? Aspectos a considerar desde la etiología del delito electrónico

Armonizar lo mejor posible el sistema penal y la normativa y operatividad consecuente del Derecho social, en unión de las oportunidades ofrecidas por el resto de la Política social (...) las directrices de la Política criminal deben tener en cuenta cómo el individuo se inserta en la comunidad y cómo operan los factores favorables o contrarios a la criminalidad. El comportamiento humano, y en consecuencia, también el desviado, nacen del contacto interactivo con el medio circundante. Es fundamental, por ello, un examen pormenorizado de las condiciones ambientales en las que el ser humano despliega su personalidad para descubrir cuáles son los vínculos que, al decir de muchos estudiosos, existen entre la criminalidad y los estímulos físicos, sociológicos, culturales, que actúan dentro de una comunidad determinada (Herrero, 2007: p. 90)

Función de la política criminal

Permitir la individualización de las principales causas del delito. Y esto es posible sólo si se conocen, al menos parcialmente, los factores que lo determinan. Sólo así se puede iniciar una investigación directa con el fin de encontrar remedios específicos eficaces. En esto consiste, por lo demás, la finalidad de la política criminal (Herrero 2007: p. 90, 91)

Cita importante porque aporta conceptualmente para pensar en estrategias efectivas que disminuyan el riesgo en la comisión de este tipo de ilícitos.

La prevención del delito y la justicia penal deben ser examinadas dentro del contexto del desarrollo económico, de los sistemas políticos, de los valores sociales y culturales y del cambio social, así como dentro del

contexto del nuevo orden económico internacional (Herrero, 2007: p. 91)

La Política criminal como expresión de seguridad pública o seguridad ciudadana (Herrero, 2007: p. 92)

2.5. CIBERDELITOS

2.5.1. Teoría de la conducta en el Derecho Penal

Con el objetivo de lograr un amplio estudio de los delitos informáticos dentro de la dogmática penal, se hace necesario empezar su análisis desde la teoría de la conducta del derecho penal, razón por la cual citamos al Argentino Maximiliano Rusconi²²⁵, así:

“El concepto jurídico penal de acción funda la primera categoría con la que se enfrenta la estructuración del análisis de la conducta delictiva. (RUSCONI, M. 2009. P. 269) (...)

En primer lugar, el concepto de acción delimita en forma elocuente el ámbito dentro del cual se moviliza legítimamente el derecho penal.

Como unidad conceptual nos marca el requisito mínimo de legitimación: no se juzgan situaciones, estados, condiciones, sucesos naturales, o cualquier característica que no represente un comportamiento de un ser humano.

Este concepto entonces, posee una función político-criminal muy clara: significa una ruptura con el derecho penal de autor en favor de un derecho penal de acto. (RUSCONI, M. 2009. P. 270)”

²²⁵ RUSCONI, M. (2009). Derecho Penal Parte General. Buenos Aires: AD-HOC 2° Edición.

Analizar de esta forma las conductas informáticas dentro de la teoría finalista del delito permite un análisis de los delitos informáticos dentro del principio general del Derecho Penal conocido como principio de Acto.

2.5.2. Teoría del delito en el Derecho Penal

Al finalismo le ha correspondido una teoría diferenciada del tratamiento del error (teoría de la culpabilidad): la negación del tipo subjetivo de la tipicidad (dolo) provenía de la presencia de un error de tipo. Si este error de tipo era inevitable se excluía el dolo y la imprudencia, si era evitable se excluía el dolo y subsistía la posibilidad de la imputación bajo los parámetros del tipo imprudente (si él existía en la legislación positiva). Del mismo modo la consolidada idea de una culpabilidad como reprochabilidad (teoría normativa de la culpabilidad) dio lugar, en ese ámbito, a la posibilidad de la presencia de un error de prohibición en alguna de sus tres formas posibles (sobre la norma prohibitiva, sobre la norma permisiva y sobre los presupuestos objetivos de la causa de justificación). Si el error de prohibición es inevitable ello reconduce a la exclusión de la culpabilidad, si es evitable a su reducción (teoría estricta de la culpabilidad). (RUSCONI, M. 2009: 259-260)²²⁶

Por lo mismo, la Ciencia Jurídica, como mecanismo regulador de las relaciones sociales y de manera más exacta, atendiendo a su sentido teleológico, como prevención de posibles conflictos en la dinámica social, debe asumir como objeto de estudio los conflictos que comienzan a generarse producto del uso indebido de las TIC, un uso que atenta contra los derechos de propiedad intelectual, el derecho a la privacidad, los derechos del

²²⁶ RUSCONI, M. (2009). Derecho Penal Parte General. Buenos Aires: AD-HOC 2° Edición.

consumidor y en general una serie de conductas nuevas como el daño informático o el bloqueo de sistemas informáticos, y de otras, que si bien, se encontraban ya reguladas en Códigos Penales, ahora son objeto de ciertas modificaciones producto de los medios y el contexto en el que se ejecutan, tales como la estafa electrónica, la falsedad electrónica o usurpación de identidad, el espionaje, entre otros.

No obstante, en el Derecho penal colombiano se ha discutido sobre la atipicidad relativa y en ocasiones absoluta del delito informático, en razón a que para que una conducta sea punible precisa, por lo menos, de la tipicidad y como resulta claro, la ausencia de una regulación determinada, permite la impunidad de la conducta dañosa, al ser imposible su adecuación típica en atención al principio de legalidad y, en consecuencia, resulta imposible la aplicación de la analogía, pues, es bien sabido que en materia penal, ésta no aplica.

Veamos el siguiente argumento para ilustración: “El Dr. ALFONSO GÓMEZ MÉNDEZ²²⁷, afirma, tratándose de la analogía con aplicación al principio de legalidad, que este principio está consagrado en el artículo 29 de la Carta Política, en concordancia con el artículo primero del Código Penal, y que al ser analizado por la jurisprudencia y la doctrina nacional e internacional, presenta dos modalidades concretas: el principio de legalidad en sentido lato y el principio de legalidad en sentido estricto. Que el principio de legalidad en sentido lato a su vez se realiza a través de:

²²⁷ Fiscal General de la Nación en Colombia, en concepto rendido dentro de la sentencia constitucional C-739 de Junio 22 de 2000. en donde se habla del principio de legalidad. Magistrado Ponente Dr. Fabio Morón Díaz.
<http://www.corteconstitucional.gov.co/relatoria/2000/c-739-00.htm>; página consultada
 Febrero de 2007

- La estricta reserva legal en la creación de delitos y penas
- La prohibición de la aplicación retroactiva de las leyes penales.

El principio de legalidad en sentido estricto o principio de taxatividad, se refiere a:

- La descripción taxativa de las conductas punibles, que prohíbe la aplicación de la analogía in *malam partem*.
- La inequívoca descripción de dichas conductas y de las penas aplicables.”²²⁸

Frente a lo cual se presentan argumentos, sobre la necesidad de legislar de manera específica para el caso del fraude electrónico, puesto que, tal como lo enunciábamos la ausencia de legislación en este sentido trae como consecuencia altos grados de impunidad.

Si bien es cierto, que en varios Estados, desde finales de la década del 80, se ha intentado la creación de una regulación específica para el delito informático, consideramos que dadas las características actuales del mundo contemporáneo, se hace necesario un estatuto internacional, dado que las relaciones comerciales del mundo actual se realizan en un contexto global; por lo tanto, se hacen necesarias unas reglas de juego claras que garanticen el ejercicio de las transacciones en el comercio internacional, lo cual no será posible, sino en el marco de un acuerdo multilateral que vincule la voluntad política de todos los Estados del sistema mundial.

La unificación jurídica internacional, garantiza el ejercicio de las prácticas comerciales, puesto que día a día la contratación internacional, la

²²⁸ Fernández de Soto, María Clara, op. cit., p. 47-48.

administración de justicia y la remisión de correspondencia, son prácticas que se realizan de manera efectiva a través de la red.

El marco para el desarrollo de este tipo de iniciativa legislativa, puede encontrarse en el propósito de cooperación internacional de la Carta de la ONU; en sentido similar se han generado una serie de Convenios en temas como el terrorismo.

El uso masificado de la red, nos pone de cara a una revolución cultural, en donde las formalidades que, usualmente, descansaban en el soporte del documento escrito, ingresan a la esfera de lo virtual.

Si bien, existen tipos penales genéricos, la especificidad generada por el desarrollo tecnológico y científico hace necesario una legislación aplicable al caso particular, habida cuenta de los requisitos *intuitu personae* que exige la legislación penal y, en general el derecho punitivo, en cuanto a que la sanción involucra el patrimonio y la libertad de las personas. El derecho punitivo no admite la tipicidad social por cuanto se involucran derechos de los individuos y de las instituciones.

El deber ser del derecho, es la consecución de un orden social justo, por lo tanto, una adecuada regulación de las dinámicas que se generan como consecuencia de los avances en Ciencia y Tecnología permiten mantener o, al menos propender por mantener, un equilibrio en las relaciones sociales.

En ese sentido, las TIC son en la actualidad una de las herramientas más utilizadas para agilizar los trámites y comúnmente en la realización de diversas

actividades, que en el pasado retardaban los procesos. No obstante, su uso también es objeto de actividades ilícitas que desestabilizan el devenir de las sociedades. Términos como *delito electrónico*, *cybercrimen*, *fraude electrónico*, *hakcer*, entre otros, han entrado a engrosar la lista de nuevas palabras en el léxico nacional e internacional y a ser tipificados en algunas legislaciones nacionales. Sin embargo, se adolece de una estrategia coactiva internacional, que prevenga de manera eficiente este nuevo tipo de actividades ilícitas.

En ese sentido, se debe precisar que, si bien el tema del fraude electrónico hace parte de la agenda internacional, son presentados argumentos a favor y en contra de una legislación internacional, intento realizado por los Estados Partes del Consejo de Europa, a través del *Convenio sobre Cybercrimen* firmado en Budapest el 23 de noviembre de 2001, el cual tiene por finalidad regular y proscribir este tipo de conductas.

2.5.3. Desarrollo histórico del Delito informático

En este aparte veremos un breve resumen de los numerales anteriores, donde desde la óptica social y económica se encuentra el nacimiento de los delitos informáticos, para terminar en sus consecuencias de tipo jurídico, para lograr este objetivo hemos citado la obra *Delincuencia informática y fraudes Informáticos* del autor ROVIRA DEL CANTO, E. (2002):

“Hemos visto que el inicio de la introducción de los ordenadores en determinados ámbitos sociales tuvo lugar por la década de

los años 50²²⁹, pero no fue hasta al cabo de unos años, ya en los 60 cuando aparecieron, principalmente en Alemania y en Estados Unidos, los primeros artículos y publicaciones sobre casos conocidos de abusos informáticos (manipulaciones de ordenadores, de sabotaje de programas informáticos, de espionaje de datos informáticos, e incluso de uso ilegal de sistemas informáticos), esto es, manifestaciones del nuevo fenómeno de la criminalidad informática, cuya entidad y sustantividad propia ya fue discutida por la doctrina²³⁰.

Y hemos expuesto anteriormente la evolución de la incidencia de la criminalidad informática hasta llegar a la actual sociedad global del riesgo y de la información, y cómo las primeras nociones de la misma se efectuaban desde una consideración o perspectiva profundamente criminológica y no tanto penal substantiva, habida cuenta la ausencia de figuras penales específicas y la problemática adecuación de los nuevos comportamientos abusivos e ilícitos a las figuras tradicionales. Pero también es cierto que la delimitación conceptual de tal fenómeno se había venido efectuando, al principio y en la mayoría de los casos, de

²²⁹ Por aquella época se utilizaba el término computadora, de la traducción directa y textual del inglés «computer» que, no obstante, se sigue utilizando en el derecho comparado. Ha habido algunos intentos en nuestra doctrina de cambios de terminología, e incluso de modificar el término actual de ordenador, como por ejemplo por el de elaborador electrónico (GUERRA BALIC, J.: «Consideraciones para la regulación penal del delito informático», pág. 3; Comunicación presentada a la 6ª Ponencia «Delitos informáticos» de las 1 Jornadas «Abogacía e Informática» organizadas por el Il. Colegio de Abogados de Barcelona, los días 7 y 8 de mayo de 1993), pero sin que hayan prosperado. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 57.

²³⁰ Así ya entonces en la República Federal de Alemania, BETZI: «Computer- kriminalität - Dichtung und Wahrheit», Datenverarbeitung in Steuer, Wirtschaft und Recht, 1972, pág. 317, o VON ZUR MÜHLEN: «Computerkriminalität - Gefahren und Abwehr», 1973, págs. 52 y ss.; y en los EE.UU., PARKER/NYCUM/OÜRA: «Computer Abuse», 1973, págs. 86 y ss. o en el posterior análisis comparativo de TABER, J.K .. : «A survey of computer crime studies», Computer and Law Journal, 1980, págs. 275 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 57.

manera o forma simplista o muy elemental, desde la perspectiva del ámbito de investigación concreta en el que el autor en cada caso analizaba la incidencia o vinculación de la informática en su campo, y, en el ámbito del derecho penal, normalmente desde una perspectiva limitada en relación a la afectación de bienes jurídicos tradicionales.

Los primeros estudios empíricos del delito informático o delito vinculado a la informática se llevaron a cabo a partir de mediados de los años 70, aplicando métodos científicos de investigación criminológica²³¹.

Estos trabajos y estudios se centraban en el ámbito de la delincuencia económica, y principalmente referidos a la comisión de actos defraudatorios mediante la utilización o aprovechamiento de medios o sistemas informáticos. Los mismos mostraron la existencia de un número limitado de casos verificados de ilícitos informáticos, analizando algunos de cierta espectacularidad y resonancia, por aquel entonces, en el ámbito económico y social internacional, como el caso de fraude en la Fundación American Equity que integró manipulaciones de 56.000 reclamaciones de seguros por un valor de al menos 30 millones de dólares, ascendiendo en 1973 las reclamaciones por compensación de seguros entre el billón y los 2 billones de

²³¹ Así en la República Federal de Alemania el trabajo de SIEBER: «Computer- kriminalität...», cit.; en Suecia el informe de SOLARZ: «Computer Technology and Computer Crime», Report núm. 8 of the Research and Development Division, National Council of Crime Prevention, 1981; y más adelante para las Comunidades Europeas el informe de la EUROPEAN COMMUNITIES INFORMATION TECHNOLOGY TASK FORCE, «The Vulnerability of the Information-Conscious Society», de 1984. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 58.

dólares²³², el caso del Banco alemán Herstatt, relativo a transacciones especulativas cambiarias exteriores totalizando varios miles de millones dólares, y que no fueron grabadas en los archivos de cuentas del citado banco, que quebró en 1974 y causó pérdidas a sus clientes por un importe cercano a los mil doscientos millones de marcos alemanes²³³, o las manipulaciones informáticas en la empresa automovilística sueca Volvo²³⁴; pero al mismo tiempo pusieron de manifiesto la existencia de un estimable y elevado número de casos no detectados o denunciados, hecho que se constituirá, como veremos, en una de las características principales de esta categoría delictual (la denominada cifra negra). Por ello las primeras concepciones de la criminalidad informática venían enfocadas desde el ámbito penal económico. Así inicialmente TIEDEMANN²³⁵, consideraba la «criminalidad mediante computación» como una de las formas de criminalidad económica neutrales, es decir, aquellas que surgen en cualquier sistema económico con independencia de la naturaleza del mismo, y por ello procede a su estudio como reflejo de la criminalidad económica, aludiendo a la parte de aquélla que

²³² Caso recogido por LOEFFLER: «Report of the Trust y of Equity Funding Corporation of Arnerica», 1974; por SOBBEL y DALLOS: «The Impossible Dream», 1975, y cit. por SIEBER: «Legal Aspects...», cit., pág. 18. Ver el caso con más detalle en el Apartado 111.5.4.5, nota 350, ut infra. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 59.

²³³ SIEBER: «Computerkriminalität...», cit., 2ª edición de 1980, págs. 61 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 59.

²³⁴ Recogidas en el Informe Nacional Sueco presentado al XIII Congreso Internacional de Derecho Comparado y expuesto por SOLARZ: «Computer Technology and the Transformation of Criminality», Strömhoim/Hemström ed., 1990, págs. 285 y SS., y 292 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 59.

²³⁵ TIEDEMANN, K: «La criminalidad económica como objeto de investigación», en Cuadernos de Política Criminal, núm. 19, 1983, pág. 173. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 59.

perjudica los intereses patrimoniales, y no refiriéndose en absoluto a otros aspectos de la misma, como el afectante a la intimidad.

El enfoque público y científico del delito informático cambió en los 80, cuando la prensa y los medios de comunicación en general se fueron haciendo eco de asombrosos casos acerca de acceso ilegal (Hacking)²³⁶, y de «virus» y de «gusanos» informáticos²³⁷. Además, el auge de la piratería de programas informáticos, las manipulaciones en los cajeros automáticos para la obtención de dinero en efectivo y los abusos de los sistemas de telecomunicación revelaron al público en general la vulnerabilidad de la actual sociedad y también la necesidad de nuevas estrategias para la prevención, control y sanción de estos ilícitos. Se tuvo ya también constatación de que la criminalidad informática no quedaba limitada al delito vinculado a intereses económicos, sino que incluso ataca todo tipo de intereses, tal como la manipulación del sistema informático de un hospital o las infracciones informáticas de la intimidad de las personas, lo cual originalmente había sido analizado y debatido separadamente del entorno conceptual del «delito informático».

²³⁶ El peligro del «hacking» se hizo especialmente evidente en la República Federal de Alemania en 1989 cuando fueron descubiertos e incursos en procedimientos penales de dicho país «hackers» alemanes que estaban usando redes internacionales de datos para obtener el acceso a información dentro de sistemas informáticos americanos, británicos, y de otros países extranjeros, y vender sus hallazgos al anterior servicio secreto Soviético, el «KGB». Sobre el caso se publicaron las obras de AMMANN, LEHNHARD, MEIFINER, Y STAHL: «Hacker für Moskau», 1989, y STOLI: «The Cuckoo's Egg», 1989; y lo recogen también HAFNER y MARKOFF: «Cyberpunk», 1991, págs. 139 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 60.

²³⁷ Por esta misma época tuvo lugar la utilización de uno de los primeros «gusanos de Internet», creado por un estudiante americano que afectó y bloqueó cerca de 6.000 sistemas informáticos dentro de la red Internet en solamente unos cuantos días. Caso recogido también por HAFNER y MARKOFF, últ. op. cit., págs. 251 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares. P. 60.

Así, a nivel internacional, se formularon conceptualizaciones con propósitos más globales y teniendo como base principal las formas o ámbitos sobre los cuales se manifestaba tal criminalidad, incidiendo en el aspecto de la utilización de los medios informáticos para la comisión de los actos ilícitos. Así, por ejemplo TIEDEMANN²³⁸ evolucionando en sus iniciales conceptualizaciones al respecto, sostenía que con la noción de criminalidad informática se designa y comprenden «todas las formas de comportamientos ilegales, y de otro lado perjudiciales a la sociedad, que se realizan utilizando un ordenador», o, en referencia a la «criminalidad mediante computadoras», que se alude a «todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos»²³⁹. Por su lado el Departamento de Justicia Norteamericano, conceptualizaba el delito informático como «cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución»²⁴⁰. O más ampliamente, como SNEYERS²⁴¹ que consideraba los delitos informáticos como «todos aquellos que se relacionan directa o indirectamente con el medio informático (ordenadores, miniordenadores,

²³⁸ TIEDEMANN: «Fraude et autres délits...», cit., cuyo título ya de por sí es significativo. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 60.

²³⁹ TIEDEMANN, K.: «Poder económico y delito», (Traducción de A. Mantilla Vilegas), Editorial Ariel, Barcelona, 1985, pág. 122. . Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 61.

²⁴⁰ Cito en ROMEO CASABONA: «Poder informático...», cit., pág. 42. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 61.-

²⁴¹ SNEYERS, A.: «El fraude y otros delitos informáticos», T.G.P., Madrid, 1990, págs. 31 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 61.

microordenadores, equipos de tratamiento de textos, redes de telecomunicación y otros equipos informáticos, software, ficheros de datos y bases de datos)», si bien tales generosas nociones fueron seria y justificadamente criticadas²⁴².

Esta y otras nociones se ceñían a criterios tradicionales, y daban incluso lugar a clasificaciones simplistas como la desarrollada desde el punto de vista de la vinculación del fenómeno informático a la actividad delictiva tradicional, y que distinguían entre los supuestos en los que «lo informático» era el objeto del delito, de aquellos supuestos en los que «lo informático» era el medio comisivo del delito. Pero el fenómeno de la criminalidad informática ha ido evolucionando con la propia sociedad y sus cambios de paradigmas, no pudiendo ya simplificarse sus diversas modalidades comisivas o de manifestación, en aquellas clasificaciones simples y genéricas²⁴³.

Así, se fue evolucionado en la conceptualización del delito informático, y que una noción del mismo había de ser establecida como un concepto amplio, no sólo económico

²⁴² Así por ejemplo por LE STANC/VIVANT: «Lamy Droit de L'Informatique», París, 1986, pág. 8, o TORTRAS, C: «La informática y el derecho», comunicación presentada a la 6ª Ponencia sobre «Delitos informáticos» de las I Jornadas «Abogacía e Informática» organizadas por el Il·ltre. Colegio de Abogados de Barcelona, pág. 120, siguiendo a los anteriores, y que consideran que esta definición olvida que las relaciones accesorias con la técnica informática, como el robo de un ordenador, no justifican el que se pueda calificar dicho comportamiento como delito informático. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 61.

²⁴³ De hecho, como sostiene ÁLVAREZ-CIENFUEGOS SOTO, siguiendo al profesor LOSANO, todos los ilícitos tradicionales se pueden cometer mediante un ordenador o, también, pueden tener como objeto propio un ordenador (ÁLVAREZ-CIENFUEGOS SOTO, J.M.: «Informática i Dret penal. Els delictes relatius a la informàtica», en «El Codi Penal de 1995: Part especial», Studia jurídica, vol. 13, Centre d'Estudis jurídics i Formació Especialitzada del Departament de justícia de la Generalitat de Catalunya, Barcelona, 1997, págs. 191 a 209. Esta cita concretamente pág. 194 al tratar de la dimensión penal del fraude informático). Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 62.

patrimonial, y en el que, más tarde en los años 90, se ha venido a incluir también la distribución de materias o contenidos ilegales a través de Internet y el uso de ordenadores y sistemas de comunicación por grupos criminales organizados.

En 1983 un grupo de expertos de la OCDE definieron el término «computer crime» (o «computer-related crime») como cualquier conducta antijurídica, antiética, o no autorizada, relacionada con un procesamiento automático de datos y/o transmisión de datos²⁴⁴, y la amplitud de este concepto se consideró ventajosa, siendo incluso asumida por gran parte de la doctrina, como RUIZ VADILLO²⁴⁵ al permitir el uso de la misma hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, y legales. Ahora bien, lo cierto es que, se reitera, cada Uno de los iniciales estudios que se elaboraban sólo se ocupaban de aquellos fenómenos de la criminalidad informática que incidían en los problemas específicamente informáticos en su respectiva disciplina²⁴⁶. Más tarde a finales de los ochenta y principios de los noventa, otros estudios fueron desarrollando conceptos más amplios sobre el que ha venido a denominarse delito de datos y/o información²⁴⁷, y que es propiamente lo que

²⁴⁴ Ver los trabajos auspiciados por la OCDE en el apartado V.I.I ut infra. Similar traducción es la recogida por MIR PUIG en «Delincuencia informática», cit., pág. 66. y por CORREA y otros: «Derecho informático», Ed. Depalma, Buenos Aires, 1994, pág. 295. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 62.

²⁴⁵ RUIZ VADILLO, E.: «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica», Poder judicial, Número especial IX, 1989, págs. 53 a 79, concretamente págs. 58 y 59. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 62.

²⁴⁶ Otros primeros intentos de definición pueden encontrarse en GUTIÉRREZ FRANCÉS: «Fraude informático y...», cit., págs. 53 a 58. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 62.

²⁴⁷ En tal sentido BLOMM y BECKER: «Spectacular Computer Crimes», 1990, págs. 69 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 63

constituye el término actual de delito informático.

No obstante en la actualidad, y sobre todo en nuestra doctrina patria, que como siempre suele ir a remolque de la evolución dogmática en otros países y de sus reformas legislativas, con un retraso de entre cinco y diez años, siguen utilizándose mayoritariamente concepciones limitativas o parciales del «delito informático». Así por ejemplo, la clásica conceptualización de CAMACHO LOSA²⁴⁸ como «toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aún cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas», ha seguido siendo utilizada por parte de la doctrina para la elaboración de sus propias conceptualizaciones; o más actualmente la caracterización dada por CHOCLAN²⁴⁹ a la criminalidad informática, al afirmar su especificidad «por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial». O desde la perspectiva del denominado Derecho informático, las de DAVARA²⁵⁰ que lo define como «la realización de una acción que, reuniendo las características que delimitan, el concepto de

²⁴⁸ CAMACHO LOSA: «El delito...», cit., pág. 17. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 63

²⁴⁹ CHOCLAN MONTALVO: «Estafa por computación...», cit., pág. 1070. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 63

²⁵⁰ DAVARA RODRÍGUEZ: «Manual de...», cit., si bien inicialmente niega la existencia como tal del delito informático (pág. 286), posteriormente, acepta tal expresión (pág. 288). Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 63

delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software», refiriéndose, por lo demás, solamente a la comisión de un delito por medios informáticos y/o telemáticos, como en similares términos PÉREZ LUÑO²⁵¹; o la de GÓMEZ PERAL²⁵² como «conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos». (ROVIRA del CANTO, E. 2002. P. 57-64”)

2.5.4. Concepto de delito informático

En esta suerte, el desarrollo de la ciencia y la aplicación, desde la tecnología, ha permitido el desarrollo de disciplinas como la Informática, que facilitan el desarrollo de diversas actividades, tanto empresariales como cotidianas; “es importante destacar (...) que la informática constituye en nuestros días el sector más dinámico de la economía mundial, ostentado una elevada tasa de crecimiento anual, equivalente al 18%”²⁵³; sin embargo, este avance del ingenio del ser humano, es objeto de conductas disvaliosas como el *haking*,

²⁵¹ PÉREZ LUÑO, A.E.: «Manual de Derecho e Informática», Barcelona, 1996. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 64.

²⁵² GÓMEZ PERAL, M.: «Los Delitos Informáticos en el Derecho Español», 4ª Ponencia presentada en la mesa núm. 5 «Delitos informáticos» en el III Congreso Iberoamericano de Informática y Derecho, celebrado del 21 al 25 de Septiembre de 1992 en Mérida (Badajoz), Informática y Derecho núm. 4, «Actas del III Congreso Iberoamericano de Informática y Derecho», Vol. I. U.N.E.D. (Centro Regional de Extremadura) / Editorial Aranzadi, Mérida, 1994, pág. 482. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 64.

²⁵³ Altmark, Daniel Ricardo, La etapa precontractual en los contratos informáticos, Departamento de Postgrado facultad de derecho, Universidad de Buenos Aires, p. 1(documento electrónico). p. 5.

entendido como el acceso ilegítimo informático; el *cracking*, destrucción o daño de la información en medio informático, entre otras conductas posibles como el espionaje, el sabotaje o el fraude informático.

Por lo tanto, la disciplina jurídica ha tenido que ocuparse de este problema para que, a través de la ley, el ordenamiento penal enfrente aquellas conductas que ponen en riesgo la tranquilidad y el continuo devenir de una sociedad globalizada; en otras palabras, la informática, no es entendida aquí como instrumento al servicio del derecho; por el contrario se convierte en objeto del derecho, que es preciso analizar con la finalidad de ofrecer respuestas y garantías sociales. “Tradicionalmente se había considerado que la función del Estado en el ámbito de la penalidad, se reducía a garantizar la seguridad y el bienestar de los asociados, aislando del conglomerado humano a elementos nocivos que con su comportamiento ilícito hubiesen lesionado o puesto en peligro intereses individuales o sociales jurídicamente protegidos; hoy se reconoce que la función del ordenamiento jurídico-penal es de más amplio alcance, pues no solamente se limita a asegurar las condiciones fundamentales de la vida en común, sino también a “promover el desarrollo y el mejoramiento de la sociedad”²⁵⁴.

Pues bien, podemos plantear entonces que la problemática del delito informático se presenta en dos casos: de un lado ubicando la informática como medio utilizado para la consumación del delito, o como objeto de efectivización de una conducta disvaliosa; cualquiera de los dos supone un factor criminológico que asciende en importancia, de lo cual resulta necesario la estructuración de tipología y regulaciones específicas, como se plantea en el

²⁵⁴ ANTOLISESI Francesco, citado en: REYES, A. (1972) “Derecho Penal, Parte General”, Bogotá D.C.: 2da edición, Publicaciones Universidad Externado de Colombia, pág. 5.

siguiente ejemplo: El Instituto Suizo de Seguro informaba que las compañías aseguradoras sufrían pérdidas anuales equivalentes a los cuatro mil millones de francos, emergentes de los denominados delitos informáticos. En Francia, en 1984, el resultado de los diferentes tipos delictuales vinculados a la informática, ascendió a la suma de setecientos millones de francos; al realizar un estudio comparativo se encontró que esta circunstancia era diez veces mayor a los asaltos tradicionales a bancos efectuados en toda Francia durante el mismo período²⁵⁵.

Entonces, y siguiendo a Erick Iriarte, toda una autoridad en esta nueva etapa del derecho, se precisa de una regulación, ya que, si bien existen fenómenos que se encuentran regulados, o a los que les son aplicables normatividades existentes, “(...) hay temas nuevos que requieren ser regulados, los delitos que afectan el bien jurídico información tienen que ser establecidos, el documento digital como medio probatorio tiene que ser contemplado en el código procesal civil, pero también el uso de medios digitales para la declaración de la voluntad. Un trabajo de adecuación normativa a una realidad”²⁵⁶.

No obstante, dicha regulación no puede ser entendida sin la elaboración de una política criminal adecuada, que sustente filosóficamente la norma jurídica, más aún, que integre políticas sociales de desarrollo, de Estado, teniendo en cuenta los componentes de las TIC's, con la finalidad de construir unas

²⁵⁵ Altmark, Daniel Ricardo, La etapa precontractual en los contratos informáticos, Departamento de Postgrado facultad de derecho, Universidad de Buenos Aires, p. 1(documento electrónico). p. 7

²⁵⁶ Iriarte Ahon E. (2005), “Sociedad de la información: Políticas y Regulación en América Latina y el Caribe ¿Hacia dónde vamos los profesionales del derecho y las nuevas tecnologías?”, AR: Revista Derecho Informático, ISSN 1681-5726, Ed. Alfa Redi, No. 089, Diciembre de 2005, página consultada febrero 2007.

políticas de Estado integradas, producto de decisiones estratégicas de cara a las necesidades y los retos de la sociedad de la información.

Es así, como aparece lo que para un sector de la doctrina se denominará el *delito informático*, como una nueva tendencia para la comisión de ilícitos en la sociedad, es decir, el empleo de la informática con ánimo doloso o culposos, conducta que comienza a ser objeto de tipificación penal como intervención positiva del Estado, con la finalidad de cumplir con sus fines esenciales; sin embargo, en el marco de la sociedad internacional se precisa abrir la discusión frente a un derecho penal sancionador, no solamente desde la óptica local, sino con una concepción desde el derecho internacional²⁵⁷.

En ese mismo sentido, el Profesor argentino Hugo Carrión, al hacer referencia al cambio en la estructura social por la masificación del internet, señala que dicha evolución tiene un aspecto negativo; “en efecto, la informática ha abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. Y a ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.”²⁵⁸

Así mismo, se debe afirmar que el uso de las TIC`s, no se limita al ejercicio de actividades en procura del bienestar social; el mismo objeto se presta para la ejecución de delitos tradicionales, pero empleando mecanismos no convencionales, producto del desarrollo de la tecnología; en otras palabras,

²⁵⁷ Iriarte Ahon, E. (2005), “Sociedad de la información: Políticas y Regulación en América Latina y el Caribe ¿Hacia dónde vamos los profesionales del derecho y las nuevas tecnologías?”, AR: Revista Derecho Informático, ISSN 1681-5726, Ed. Alfa Redi, No. 089, Diciembre de 2005, página consultada febrero 2007.

²⁵⁸ Carrión Zorzoli Hugo, *Op. Cit.*

realización de ilícitos mediante herramientas informáticas, dando lugar a la necesidad de tipos legales autónomos que así lo justifiquen. Frente a este punto específico encontramos varias escuelas, una de ellas justificada por el criterio de Gabriel Campoli, quien considera que no se precisa de la tipificación de nuevos delitos, en razón a que adolecen de la característica: nuevo; no son nuevos, son los mismos que ya están tipificados excepto, que su comisión se realiza a través de otros medios.

2.5.5. Naturaleza de los delitos informáticos

CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H ya se han pronunciado frente a los cambios necesarios en la realidad jurídica de los Estados que permiten tipificar los delitos informáticos teniendo en cuenta su naturaleza, que aunque no es nueva en el mundo, su comisión si es objeto de estudio de forma muy reciente en relación a los delitos tradicionales, lo que conlleva a la creación y discusión de nuevas teorías jurídicas.

Una de las grandes dificultades en este aspecto la viven los países de tradición jurídica Romano Germánica, donde procedimentalmente no es viable la adecuación de la Ley al mismo ritmo que avanza, cambia y se desarrolla la tecnología fuente de la comisión de delitos informáticos.

Teniendo en cuenta lo anterior se hace necesario citar a CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H. al respecto.

El fenómeno de los delitos de alta tecnología y relacionados con las redes informáticas requiere la tipificación de delitos totalmente nuevos y la modificación de los tipos de delitos existentes para garantizar que se apliquen a la utilización abusiva de las nuevas tecnologías. “Es de

remarcar el positivo avance que constituye contar con normas específicas que tipifiquen las acciones que, hasta su sanción, estaban exclusivamente bajo la interpretación de los jueces para cada caso particular que se les presentaba²⁵⁹. Por otro lado, sostenemos que si bien el objetivo principal -contar con legislación adecuada en el tema- está cumplido²⁶⁰, es necesario contar con una constante actualización, tanto a nivel técnico, legislativo, como jurisprudencial, dada la constante evolución que se verifica en el ámbito de las tecnologías de la Información y Comunicaciones, donde un día estamos actualizados y el siguiente esa información es obsoleta”.

Está surgiendo un consenso internacional con respecto al núcleo esencial de los comportamientos más graves y perjudiciales, pero quedan algunas esferas que algunos Estados consideran delitos, pero no todos. Los dos ejemplos principales son los problemas de propiedad intelectual, como la copia no autorizada de programas informáticos o de datos, y el problema de qué es lo que se denomina contenido ofensivo. La explotación delictiva de las nuevas tecnologías ha llevado a formas totalmente nuevas de delito. En otros casos, formas de delito más tradicionales se cometen de nuevos modos que aumentan los beneficios o disminuyen los riesgos para los delincuentes. Una tercera categoría básica de actividad delictiva consiste en la utilización más general de las tecnologías por los delincuentes para organizar, comunicar y proteger de la vigilancia sus actividades. Entre otras

²⁵⁹ MARTINEZ FAZZALARI, Raúl, “Sobre la reciente ley de delitos informáticos”. Disponible en <http://portal.educ.ar/debates/sociedad/sobre-la-reciente-ley-de-delit.php>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 119.

²⁶⁰ Delitos informáticos: aseguran que la ley es “muy positiva”, pero advierten que necesitará “adecuación”: Para el fiscal Ricardo Sáenz, la ley “inserta a la Argentina en el concierto de las naciones civilizadas del mundo” y obliga a los jueces y fiscales a capacitarse constantemente. Disponible en <http://www.clarin.com/diario/2008/06/05/um/m-01687769.htm>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 119.

esferas básicas de clasificación propuestas se encuentra la clasificación según silos delitos se cometen por los delincuentes para obtener ganancias económicas o materiales o por otros motivos, y si esos delitos implican otros delitos cometidos contra sistemas informáticos o de comunicaciones, o la utilización de esas tecnologías para hacer víctimas a otras personas²⁶¹. (CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H. 2009. P. 119-120)

2.5.6. Bienes e intereses jurídicos protegidos en el delito informático

Al hacer referencia al delito informático, precisa que los bienes jurídicos que se encuentran en riesgo y que ameritan de protección ya están regulados, como por ejemplo el honor, la protección de datos, el patrimonio, por lo tanto lo que se necesita es una adecuada interpretación de la norma penal. “Determinado el bien jurídico protegido, podremos inducir que, en el caso de los delitos informáticos, los múltiples posibles ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales.”

“¿Entonces qué es lo que nos separa de una correcta aplicación de las leyes penales preestablecidas? Sólo la pretendida falta de legislación en materia de

²⁶¹ Naciones Unidas, “Conclusiones del Estudio sobre medidas eficaces para prevenir y controlar los delitos de alta tecnología y relacionados con las redes informáticas”, Comisión de Prevención del Delito y Justicia Penal, 10° período de sesiones Viena, 8 a 17 de mayo de 2001, Tema 4 del programa provisional, Cooperación internacional en la lucha contra la delincuencia transnacional. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 120

delitos informáticos, y digo pretendida, porque esto no es así, ya que al perpetrarse el delito a través del uso de medios informáticos no se está sino en presencia de un nuevo método comisivo del delito y no, como erróneamente se piensa, de un nuevo delito que para que lo sea, debe estar correctamente tipificado.

“En resumen, los delitos informáticos, en su gran mayoría, dependen para su persecución penal de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces, de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, por ejemplo, que si mañana se pudiese quitar la vida a alguien por medio de internet, habría que establecer una nueva figura penal ya que el homicidio no estaría cubriendo esta posibilidad; cuando en Derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica”²⁶².

Ahora bien, señala que debe realizarse una rotunda diferencia entre delito electrónico e informático, en razón a que si existen una serie de conductas que hasta el momento no se encuentran tipificadas como el hacking; no obstante, considera que este debe enmarcarse como un delito electrónico y no informático, dado que el mismo no posee a primera vista un bien jurídico tutelado.

Así las cosas, nos parece conveniente precisar la diferenciación realizada por el Profesor Campoli:

²⁶² CAMPOLI, G.A. (2002) “Hacia una correcta Hermenutica Penal - Delitos Informáticos vs. Delitos Electrónicos”, No. 048 - Julio del 2002, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi. <http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>, Página consultada marzo de 2007

“Delitos Informáticos: Son todos aquéllos en los cuales el sujeto activo, lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, por medio de la utilización indebida de medios informáticos.

“Delitos electrónicos o informáticos electrónicos: son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios”²⁶³.

En conclusión, se puede decir, según el criterio del Profesor Campoli, que la característica diferencial entre delito informático y delito electrónico, es que del primero, ya existe la tipificación de la conducta disvaliosa, así como la protección del bien jurídico tutelado; lo que ocurre es que los medios para la comisión del ilícito son otros diferentes a los previstos por el legislador, y en cuanto al delito electrónico, al ser perpetrado a través de medios informáticos, se convierte en una especie de género de los informáticos.

Entonces retomemos; hasta el momento hemos, señalado que el empleo de la informática ha influenciado en los cambios estructurales de la sociedad y que, a la par han aparecido conductas que se valen de los adelantos tecnológicos con fines criminales y que ante este uso disvalioso del avance del ingenio humano, se presenta una ambivalencia en cuanto al término para

²⁶³ CAMPOLI, G.A. (2002) “Hacia una correcta Hermenutica Penal - Delitos Informáticos vs. Delitos Electrónicos”, No. 048 - Julio del 2002, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi. <http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>, Página consultada marzo de 2007

englobar ese tipo de ilícitos, delito informático o delito electrónico y precisamos una salida ofrecida por el Profesor Campoli.

Ahora bien, existen diferentes términos conceptuales para definir estas conductas; José Cuervo realiza una sistematización de las principales, veamos:

“a) Delincuencia informática

La define GÓMEZ PERALS como conjunto de comportamientos dignos de reproche penal, que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

“b) Criminalidad informática

ALESTUEY prefiere hablar de “delincuencia o criminalidad informática”.

BAÓN RAMÍREZ²⁶⁴ define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

TIEDEMANN considera que con la expresión “criminalidad mediante computadoras”, se alude a todos los actos, antijurídicos según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos.

²⁶⁴ BAÓN RAMÍREZ, R. (1996) *"Visión general de la informática en el nuevo Código Penal"*, en *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, Madrid: Escuela Judicial/Consejo General del Poder Judicial, págs. 77 a 100.

“c) Delitos informáticos

ROMEO CASABONA²⁶⁵ se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Para DAVARA RODRÍGUEZ no parece adecuado hablar de Delito Informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal, para que pueda existir un delito. El Código Penal de 1995 no introduce el delito informático ni admite que exista como tal un Delito Informático, si bien admite la expresión por conveniencia, para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático. Define el Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.

PARKER define los Delitos Informáticos como todo acto intencional, asociado de una manera u otra a los ordenadores, en los cuales la víctima ha o habría podido sufrir una pérdida y cuyo autor ha o habría podido obtener un beneficio.

²⁶⁵ ROMEO CASABONA, C. M. (1996). *"Delitos informáticos de carácter patrimonial"*, Informática y Derecho nº 9,10 y 11. Mérida: UNED, Centro Regional de Extremadura. P. 413-412.

“d) Computer crimen

En el ámbito anglosajón se ha popularizado la denominación de “Computer Crime” y en el germano la expresión “Computerkriminalität”

“e) Delincuencia de cuello blanco

La doctrina, casi unánimemente, la considera inscribible en la criminalidad “de cuello blanco”

Para SUTHERLAND, la delincuencia de cuello blanco es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.

“f) Abuso informático

RUIZ VADILLO recoge la definición que adopta el mercado de la OCDE en la Recomendación número R (81) 12 del Consejo de Europa, indicando que Abuso Informático es todo comportamiento ilegal o contrario a la ética o no autorizado, que concierne a un tratamiento automático de datos y/o transmisión de datos.

La misma definición aporta CORREA incidiendo en la Recomendación (89) 9, del Comité de Ministros del Consejo de Europa, considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países, respecto a la delincuencia relacionada con el ordenador”²⁶⁶.

Finalmente, podemos realizar una caracterización del Delito Informático señalando que es “aquél que directa o indirectamente se relaciona con un

²⁶⁶ Cuervo, José, (1999) “Delitos informáticos: protección penal de la intimidad”, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi, No. 006 – Enero del 1999., <http://www.alfa-redi.org/rdi-articulo.shtml?x=207> página web consultada abril 2007.

sistema computarizado como medio u objetivo en la realización del mismo. A título enunciativo, pueden mencionarse los siguientes tipos, entre otros:

- Venta a terceros de sistemas y programas de propiedad de la empresa.
- Robo de archivos con información confidencial
- Uso o venta no autorizada de servicios y equipos.
- Chantaje o extorsión.
- Sabotaje o vandalismo contra instalaciones y equipos.
- Fraude financiero
- Modificación no autorizada de archivos o programas.²⁶⁷

Según la propuesta del Juez Alexander Díaz en el proyecto de ley analizado en el capítulo cuarto, se retoman estas conductas.

Según la investigación realizada en España por la firma *Landwell, Abogados y Asesores Fiscales* durante el primero de enero de 2001 al 31 de diciembre de 2003, bajo el título de *Actos desleales de trabajadores usando sistemas informáticos e internet* se concluyó, de 393 casos estudiados, que las infracciones más habituales son: la creación de empresa paralela, utilizando activos inmateriales de la empresa; daños informáticos y uso abusivo de recursos informáticos; información confidencial y datos personales; amenazas, injurias y calumnias; infracción de propiedad intelectual e introducción de obras de la empresa en redes P2P²⁶⁸; intercambio de obras

²⁶⁷ Cfr. Delpiazzo Carlos, Eirin Álvaro, Montano Pedro, *Aplicación del derecho a la informática*, Departamento de Postgrado, Facultad de Derecho, Universidad de Buenos Aires, p. 9 (documento electrónico).

²⁶⁸ “Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros. En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros (peer to peer)”. Ribas Javier, director del estudio, y otros,

de terceros a través de redes P2P y la infracción de derechos de propiedad industrial. Entre los aspectos preocupantes se destaca la actitud de las empresas, en razón a que con la finalidad de evitar la difusión de este tipo de conductas llegan a acuerdos con los infractores. Por ejemplo solamente el 26% de las infracciones descubiertas son llevadas ante los tribunales, contra un 74% que realiza acuerdo transaccional. En el mismo sentido solamente el 13% de las empresas deciden divulgar la existencia de este tipo de infracciones. Por el contrario, el 74% restante decide no publicitar dicha información con la finalidad de preservar su reputación; consideran que la revelación de problemas de seguridad puede generar desconfianza en el mercado²⁶⁹.

De otro lado, indican los resultados del estudio que la infracción más habitual es el intercambio de obras de terceros en redes P2P, lo cual equivale al 31% de la muestra, seguido por la creación de empresa paralela con propiedad intelectual de la empresa con un 22%. De lo anterior se desprende, tal como indica esta firma, que el sector que más resulta afectado es el del desarrollo del software con equivalente al 55%. En cuanto a las motivaciones pudo establecerse que el 51%, responde al ánimo de lucro, seguido por un 41% como resultado de un conflicto laboral o despido injusto. Vale la pena aclarar que este tipo de conductas, ha ido en aumento desde el 2001 al 2003 y que las cuantías también son importantes, por, las infracciones cometidas por los trabajadores a las empresas se estiman alrededor de los 60.000 euros. Sin embargo solamente el 3% de las infracciones analizadas generan perjuicios

Actos desleales de trabajadores usando sistemas informáticos e internet, <http://www.onnet.es/estudio001.pdf> noviembre 17 de 2010, España, 2003, p. 7.

²⁶⁹ Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros. En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros (peer to peer)". Ribas Javier, director del estudio, y otros, *Actos desleales de trabajadores usando sistemas informáticos e internet*, <http://www.onnet.es/estudio001.pdf> noviembre 17 de 2010, España, 2003, p. 7.

superiores a los 300.000 euros; además de un elemento que inestimable económicamente, como lo es la apropiación indebida de código fuente de aplicaciones informáticas y la explotación de activos inmateriales, a través de terceros o de empresas que son constituidas por los mismos trabajadores²⁷⁰.

Otro caso importante de señalar son, por ejemplo los delitos más comunes cometidos en México, a través de plataformas electrónicas: la clonación de tarjetas de crédito y el *phising* o transferencias electrónicas ilegítimas²⁷¹, éstos entre otros países.

Principio de legalidad y analogía en el delito informático

Antes de entrar a analizar la necesidad o no de una tipificación del hecho punible, en este caso del delito informático, se precisa de la delimitación del bien jurídico tutelado que resulta entonces ser la información, la cual amerita de la tutela jurídica. No obstante, “es necesario aclarar que un hecho no puede ser tenido como ilícito, mientras no aparezca descrito en un tipo legal, en donde igualmente esté señalada la pena respectiva; dedúcese (sic) de aquí

²⁷⁰ Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros. En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros (peer to peer)”. Ribas Javier, director del estudio, y otros, *Actos desleales de trabajadores usando sistemas informáticos e internet*, <http://www.onnet.es/estudio001.pdf> noviembre 17 de 2010, España, 2003, p. 18.

²⁷¹ CAMPOLI, G.A. (2002) “Hacia una correcta Hermenutica Penal - Delitos Informáticos vs. Delitos Electrónicos”, No. 048 - Julio del 2002, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi. <http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>, Página consultada marzo de 2007

que, desde un punto de vista puramente formal, es delito todo hecho humano legalmente previsto como tal y cuya consecuencia es una pena”²⁷².

En tanto, se precisa la armonización con los principios fundamentales de la dogmática penal, en ese sentido se debe aclarar de antemano la imposibilidad de aplicación de la analogía para la sanción de ilícitos que no aparecen tipificados en el ordenamiento penal, pero que guardan similitud con otras figuras como por ejemplo la estafa. En España se presentó un caso con un empleado bancario que manipuló las cuentas corrientes de varios clientes; se apropió de más de 3.000.000 pesetas. El tribunal al analizar la norma penal de la estafa la cual señalaba *que “el que con ánimo de lucro, utilizaré engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno (...)”*²⁷³ intentó realizar la adecuación típica de la conducta; sin embargo, la norma necesitaba de dos elementos claros; de un lado, la utilización de engaño bastante por el autor del ilícito y la producción de un error en la víctima. Entonces, si bien existía el ánimo de lucro no aparece el engaño a tercero y error suficientes, puesto que el autor del delito no utilizó ninguna treta ni artimaña para engañar a la víctima, para viciar la voluntad del tercero, puesto que la acción se produjo a través de una máquina, el ordenador, y como consecuencia tampoco cabe plantearse la producción de error por el mismo motivo²⁷⁴.

²⁷² REYES, A. (1972) “Derecho Penal, Parte General”, Bogotá D.C.: 2da edición, Publicaciones Universidad Externado de Colombia. p. 92.

²⁷³ Artículo 528 del Código Penal Español anterior a 1995.

²⁷⁴ Portela Calderón, Carlos y Díaz Héctor, “Delitos Informáticos”, Universidad Cooperativa de Colombia, Facultad de Derecho, 2004. p. 6, www.alediag@net.com

De tal manera, que la decisión del Tribunal que la conducta se adecuaba en una apropiación indebida, quedando imposibilitada la aplicación del tipo de estafa por analogía, para el ilícito cometido por el empleado²⁷⁵.

Finalmente, señalan los autores, “la necesidad de concurrencia de estos dos elementos ha impedido, en muchas ocasiones, poder calificar un hecho como de estafa, cuando ha tenido lugar mediante la utilización de un medio informático o cuando éste ha estado presente en la acción delictiva de cualquier otra forma. Por ejemplo, no es posible subsumir la estafa realizada por una persona, utilizando el ordenador de su casa, logrando la transferencia bancaria de la cuenta de un tercero, a una de su titularidad”²⁷⁶.

De cara a la doctrina, en el Derecho Penal colombiano, explica el maestro Reyes Echandía, no es procedente extenderla a casos no contemplados en la ley tomando como referencia otras figuras delictivas o sanciones ya previstas “*tal analogía no es de aplicación en nuestro derecho positivo porque resulta manifiestamente violatoria del principio de legalidad de los delitos y de las penas*”²⁷⁷.

Con la argumentación anterior, pretendemos reforzar la postura que se plantea en esta investigación referente a la necesidad de tipificar toda esta serie de conductas que atentan contra la armonía y la tranquilidad del conglomerado social, además porque no sería posible su sanción a través de la analogía, con lo cual lo que operaría sería la impunidad, puesto que la

²⁷⁵ Sentencia del T.S de 19 de abril de 1991, referenciada por Portela-Díaz, Op. Cit.

²⁷⁶ Portela Calderón, Carlos y Díaz Héctor, “Delitos Informáticos”, Universidad Cooperativa de Colombia, Facultad de Derecho, 2004. p. 6, www.alediag@net.com

²⁷⁷ REYES, A. (1972) “Derecho Penal, Parte General”, Bogotá D.C.: 2da edición, Publicaciones Universidad Externado de Colombia. p. 64.

requisitoria colombiana consagrada en el Código Penal es rigurosa por cuanto que exige la tipicidad, la antijuridicidad y la culpabilidad, como presupuestos básicos para que opere el mecanismo sancionador de la condena, que da lugar al resarcimiento patrimonial de los perjudicados y/o ofendidos de dicha legislación.

Ahora bien, una de las características de un Estado social de derecho, sustentado en una Constitución, es la aplicación del principio de legalidad, a través del cual se erige un dique al poder estatal para la sanción de los inculpadados, principios claramente recogidos en la Constitución Política colombiana.

Por lo tanto, se precisa de la tipificación de aquellas conductas que han sido catalogadas como atentatorias de bienes jurídicos, condición sin la cual se deviene en un Estado que retoma las prácticas de sistemas de gobierno despóticos.

La tradición de la ilustración francesa propuso como un significativo representante a César Beccaria, quién influyó en la redacción de la Declaración de los derechos y deberes del hombre y del ciudadano de 1789; *“El origen del principio de legalidad²⁷⁸, hay que hallarlo en la filosofía de la Ilustración, en aquel momento histórico en el que el pueblo pasa de ser instrumento y sujeto pasivo del poder absoluto del Estado o del Monarca que lo encarna, a controlar y participar de ese poder, exigiendo unas garantías en*

²⁷⁸ Según Francisco Puy Muñoz se atribuye a Paul Joham Asnelm Feuerbach la paternidad de las fórmulas latinas utilizadas generalmente para enunciar el principio de legalidad sustantivo: *Nulla crimen sine lege* y *Nulla poena sine legal*. Aparece en *Las fórmulas del principio de legalidad, Los derechos fundamentales y libertades públicas*, (II) Madrid, Din Impresores, S.L., 1993, Vol I, p. 504.

su ejercicio, y la idea de que ésta ley no puede ser otra que la aprobada exclusivamente por un poder legislador que represente a los ciudadanos”²⁷⁹.

Por lo mismo, el artículo 5º de la Declaración de los derechos y deberes del hombre y del ciudadano establece: “La ley no tiene el derecho de prohibir más acciones que las nocivas a la sociedad. Todo lo que no esté prohibido por la ley no puede ser impedido y nadie puede ser constreñido a hacer lo que ella no ordena”.

Entonces, el principio de legalidad consiste en una fórmula que limita y controla el poder del Estado; después del siglo XX, no solamente aparece en las Constituciones modernas, sino que, además, es retomado en los instrumentos internacionales de derechos humanos con la finalidad de imponer obligaciones a los Estados para exigir el respeto de los derechos de las personas, en razón a que solamente posee atribuciones constitucionales para crear una norma sancionatoria de dichos derechos siempre y cuando provenga del Congreso o Parlamento.

Si bien varias conductas se quedan impunes por no estar tipificadas, sería un retroceso además de constituir un absurdo jurídico, el pretender adecuarlas a otras ya existentes por aplicación de la analogía; por lo tanto se precisa de la creación de tipos penales sancionatorios de los nuevos ilícitos producto de la revolución tecnológica.

²⁷⁹ De Vicente Martínez, p. 17 citado por Ernesto Rey Cantor, “Las generaciones de los derechos humanos”, Universidad Libre, cuarta edición, ISBN 958-676-346-1 Bogotá, 2006, p. 145.

Sin embargo, otros autores plantean la interpretación extensiva como solución a la sanción de los delitos informáticos, entre ellos se encuentra el maestro español Emilio Suñe²⁸⁰, quien plantea una interpretación extensiva de los tipos penales, como propuesta para evitar que la delincuencia informática se encuentre siempre en ventaja antes que el derecho.

Plantea este autor, que existe mucho apego al principio *nullum crimen sine lege*, y no es tan necesaria la tipificación de nuevas conductas si se opta por flexibilizar los Códigos, y flexibilizar los criterios de interpretación.

Este autor comenta, que no es importante introducir nuevos tipos penales, sino el cambio de mentalidad interpretativa.

Sin embargo, la postura de este doctrinante tiene cierta reticencia en el medio, porque existe la idea de que es extremadamente difícil distinguir la interpretación extensiva de la analogía, y la falta de claridad que existe en la doctrina moderna.

Pero el mismo autor, esboza un criterio diferenciador entre analogía e interpretación extensiva, y arguye que “*El criterio diferenciador más nítido entre analogía e interpretación extensiva, estriba en que la analogía se basa*

²⁸⁰Doctor *cum laude* en Derecho (1985) por la Universidad Complutense de Madrid, ha publicado seis libros y cerca de cincuenta artículos científicos, en libros colectivos o revistas especializadas. En el ámbito de la Informática y Derecho, se destaca su libro *Informática práctica para juristas y profesionales del mundo de las letras* (1994); así como sus artículos sobre Informática Jurídica en general, bases de datos legislativas y parlamentarias, thesauri, Lógica jurídica y sistemas expertos, Management y Derecho, Derecho de la Informática en general, contratación administrativa informática, Derecho de las Telecomunicaciones y teletrabajo, entre otros.

en extraer los principios que informan la regulación de uno o varios supuestos normados, para aplicarlos después a casos que guardan identidad de razón con los previstos en aquellas normas. La interpretación extensiva, en cambio, afecta más a la disposición que a la norma propiamente dicha; pues no trata de alumbrar una nueva norma a través de la inducción de principios generales del Derecho, a partir de otra u otras normas expresas, sino de rebasar una interpretación de tipo estrictamente declarativo de una norma expresa. La interpretación extensiva no deja de ser una variedad de la literal, con el matiz de que los términos en que está redactada la correspondiente disposición se interpretan en sentido amplio y no meramente declarativo²⁸¹.

Nos encontramos entonces, con dos situaciones; por un lado la imposibilidad de aplicar la analogía, por el rígido principio de *nullum crimen sine leg*, entonces se da como solución en este caso la creación de nuevos tipos penales, y de otro lado la Interpretación extensiva que propone todo lo contrario, y posibilita la flexibilización de la norma y se da como solución a la masiva creación de tipos penales constantes, para sancionar conductas modernas delictuales, toda vez que la analogía es inoperante en el Derecho Penal.

Tipicidad del delito informático

Una vez realizada la primera gran conclusión de, por qué razón es inaplicable la analogía en la calificación de conductas atentatorias de la seguridad informática y el consecuente respeto por el principio de legalidad como

²⁸¹ Suñe Emilio, "El delito informático como motor de cambios conceptuales en el Derecho Penal", No. 040 - Noviembre del 2001, p. 03

garantía de un ordenamiento penal, justo fundamento de la seguridad jurídica, pasamos a sustentar la importancia y necesaria tipificación de los delitos informáticos.

Como quiera que la estructura del delito esté conformada por la tipicidad, la antijuridicidad y la culpabilidad, para efectos de esta investigación analizaremos la tipicidad²⁸² de los delitos informáticos y el bien jurídico, a fin de determinar la antijuridicidad.

Según el jurista colombiano Alfonso Reyes Echandía, el tipo legal es “la abstracta descripción que el legislador hace de una conducta humana reproachable y punible”²⁸³.

Ante la impunidad creciente presentada en razón a que los sistemas jurídicos no estaban preparados para el advenimiento de conductas que atentaban contra el avance de la Ciencia y la Tecnología y que se configuran como una usurpación a los derechos de propiedad intelectual, específicamente a la información y el conocimiento²⁸⁴, se precisa, por parte del Estado, de una acción contundente encaminada a la protección de dichos intereses, pero más

²⁸² Es lo que los alemanes llaman Tatbestand, los italianos fattispecie legale y los españoles tipicidad, Jiménez de Azua, citado por REYES, A. (1972) “Derecho Penal, Parte General”, Bogotá D.C.: 2da edición, Publicaciones Universidad Externado de Colombia, p. 99.

²⁸³ REYES, A. (1972) “Derecho Penal, Parte General”, Bogotá D.C.: 2da edición, Publicaciones Universidad Externado de Colombia p. 99.

²⁸⁴ El Profesor Eduardo Pastrana Ph. D., señala que “Hay una diferencia entre ambas definiciones. La información es el acopio de datos que no por sí mismos tienen organización. El jerarquizar datos y establecer relaciones entre ellos, el darles determinados sentidos, direcciones u organización es un proceso mucho más delicado. La información debe articularse en complejas estructuras cognoscitivas para convertirse en conocimiento.” Pastrana Buelvas Eduardo, Documento magnético: “Propuesta para la articulación del sistema del desarrollo de una cultura de la investigación en la facultad de ciencia política y relaciones internacionales de la Pontificia Universidad Javeriana”, Bogotá, 2006, p. 3.

que el Estado, tendríamos que hablar del conjunto de Estados y de los otros actores que conforman la sociedad mundial (fuerzas transfronterizas como las multinacionales, la IBM, la Microsoft, entre otras; las organizaciones intergubernamentales como la UNESCO, la OMC, la INTERPOL; los movimientos sociales, la opinión pública internacional, entre otros), en razón a que en un mundo globalizado ningún esfuerzo es suficiente a nivel local; se requiere por tanto de salidas globales, a través de la suma de intereses y el restablecimiento del derecho penal internacional.

De igual forma encontramos conductas delictuales globales, llamado por el maestro Suñe, “delito global”, como diferenciador de la delincuencia internacional tradicional debido a su ubicuidad, es decir que multiplica sus efectos, en aquellos aspectos en donde el delito es posible, y de la misma forma posibilita su persecución, debido a que no se encuentra delimitado por cuestiones territoriales, toda vez que no se trata de un delito cometido en un Estado determinado, sino que se parte de la realidad que se está cometiendo a la vez en todos los Estados en que se encuentre tipificado el delito, toda vez que en ellos se puede acceder a la información pertinente. Un ejemplo claro de delito global es la pornografía infantil; este se puede realizar a través de la Internet, o por medio de otras redes de transmisión de datos de carácter global; entonces, por su naturaleza no da pie para entenderse cometido el ilícito en un país concreto, si no que se entiende que se pudo realizar en todos a la vez. Al respecto dice lo siguiente: *“Los que acabo de denominar delitos globales constituyen un fenómeno de nuevo cuño, vinculado a conductas antisociales de alcance y efectos directamente universales, por cuanto que se realizan a través de las grandes redes de transmisión de datos hoy singularmente a través de Internet . Se trata de delitos tales como la difusión de pornografía infantil, o la incitación a la violencia y al odio racial, en los cuales lo de menos es en qué país radique el servidor ordenador desde el que*

se difunden tales contenidos ignominiosos y lo demás es que su difusión alcanza a la vez a todos los países del orbe, lo que sin duda los diferencia de las formas tradicionales de delincuencia internacional, que nunca tuvo semejante grado de globalidad”²⁸⁵.

Y concluye este autor con la posibilidad de aprobarse un Tratado Internacional concerniente a delitos globales, en donde se estableciera una tipificación uniforme, en la medida en que estos se vayan detectando, y la posibilidad de una competencia judicial basada en el principio de la efectividad, para evitar así, la creación de un órgano de jurisdicción internacional.

Con este marco contextual claro, encontramos que, a través de la tipicidad es posible brindar garantías jurídicas, políticas y sociales a los ciudadanos del mundo. Reiteramos, no es válido el esfuerzo local; una sociedad globalizada precisa de alternativas globales, de la suscripción, aprobación y ratificación de instrumentos internacionales que tipifiquen aquellas conductas realizadas mediante la utilización de medios informáticos, con la finalidad de castigar a aquéllos que de manera ilícita, se apropien de bienes inmateriales y que empleen las plataformas informáticas para la comisión de todo tipo de conductas proscritas socialmente.

Dichas normas condensadas en un instrumento internacional, constituirían el fundamento del tipo legal en los que se entrarían a describir los comportamientos que precisan ser elevados a la categoría de delito internacional por la lesividad que generan, incluyendo las atribuciones a las

²⁸⁵ Suñe Emilio, “El delito informático como motor de cambios conceptuales en el Derecho Penal”, No. 040 - Noviembre del 2001, p. 09

autoridades judiciales, encargadas de garantizar la lucha contra la impunidad, además de contemplar su respectiva sanción.

Bien jurídico tutelado

Párrafos atrás señalábamos, que era preciso identificar el bien jurídico objeto de la protección estatal, como condición para argumentar la necesidad de crear un tipo penal, de tal manera que se pueda igualmente establecer el límite de lo antijurídico, al determinar la medida del daño o la capacidad para atentar contra el objeto de protección.

En ese sentido, podemos decir que la necesidad de optimizar los procesos productivos para minimizar el tiempo que se representa directamente en economía de capital, el ser humano ha trabajado en el desarrollo de estrategias que le permitan garantizar la disminución de su inversión; este tipo de estrategias se pueden condensar en los logros de la revolución tecnológica.

Pues bien; el desarrollo de disciplinas como la mecatrónica, la robótica, la informática, la biotecnología, la nanotecnología, la electrónica, la ingeniería genética, la reingeniería entre otras, pretende elevar el nivel de vida de los seres humanos; por tanto, el desarrollo de la informática permite el manejo de la información de manera ágil, segura; ésta es decodificada en algoritmos para ser transportada a través de la red; diversas técnicas como la criptografía, permiten que la información sea transformada conservando la privacidad del emisor. En razón a que ésta constituye “el interés macro-social o colectivo, porque supone una agresión a todo el complejo entramado de relaciones

socio-económico culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos.”²⁸⁶

Si bien, lo que hay en juego, inicialmente, es la información como tal, esto no exige que sean afectados otros bienes jurídicos como el patrimonio por ejemplo, ya que aunque, la información aparece de manera inicial, lo que finalmente termina afectándose vulnera el patrimonio y la privacidad y la intimidad, que se encuentran erigidos en las Constituciones Políticas del mundo, entre ellas la de Colombia, como derechos fundamentales inalienables.

Pues bien; esa función del concepto de bien jurídico termina siendo la que justifica su existencia dogmática. No sólo contribuye a interpretar el objeto de la prohibición para determinar su alcance típico, sino que, permite definir el límite de lo materialmente antijurídico, por la medida del daño o la capacidad de producirlo de la conducta imputada.

Una vez esgrimidos los argumentos sobre los cuales se soporta la necesidad de la tipificación del delito informático, conviene señalar que si bien existe el Convenio sobre Cibercriminalidad, éste hace las veces de una hoja ruta, en razón a que señala la importancia de que cada Estado promueva iniciativas legislativas sancionatorias, encaminadas a frenar la impunidad del delito informático; no obstante, no es un tratado internacional autónomo, que debe

²⁸⁶ Carrion Zorzoli Hugo, “Atipicidad penal del sabotaje informático”, Revista Alfa-Redi, No. 048 – julio del 2002, <http://www.alfa-redi.org/rdi-articulo.shtml?x=1473>, ISSN 1681-5726, página consultada enero 2007. El autor participó en la redacción del Anteproyecto de Ley sobre Delitos Informáticos publicado en el Boletín Oficial 27/09/01.

recoger las legislaciones internas y por qué no, ver la posibilidad de que dichas conductas sean juzgadas por la Corte Penal Internacional, por cuanto la criminalidad informática se erige como un peligro para la humanidad en todas sus dimensiones, siendo esto tan cierto que la lucha política de los Estados y los insurgentes, se lleva a cabo en el mundo contemporáneo por este medio.

2.5.7. Características de los delitos informáticos

Rovira del Canto, en la obra citada anteriormente ha definido otra serie de características para los delitos informáticos que llevan a su identificación clara para posterior adecuación típica, antijurídica y culpable. Y no solo dentro de la dogmática penal, sino también dentro de los aspectos sociológicos y económicos del delito, así:

La Permanencia Del Hecho: Repetición Y Automatismo

Esta característica ha sido dada al delito informática por el autor Español Enrique Rovira del Canto, en su obra en cita, estableciendo:

“Efectivamente, la incidencia de la posibilidad de repetición de una actuación ilícita en el ámbito informático, favorece su nueva comisión, incluso en múltiples ocasiones, derivando en la práctica a que en un alto porcentaje de los supuestos conocidos y enjuiciados de ilícitos informáticos la conducta de los autores no se ha limitado a una única acción delictual, sino a una reiteración continua de la misma. Ello, desde el punto de vista

penal sustantivo, se plasma en lo que ALASTUEY DOBON²⁸⁷ denomina como «efecto continuado» propio de esta delincuencia, y el que por la jurisprudencia se aprecie en un alto porcentaje de ocasiones la figura del delito continuado para la sanción de tales comportamientos²⁸⁸.

Pero es que, además, cabe la realización de una sola inicial acción por parte del sujeto activo, consistente en una manipulación del programa de funcionamiento informático, o un cambio en la base de datos, es decir afectar a las funciones de almacenamiento, procesamiento y transferencia de datos o de la información, para que la frecuente repetición del hecho delictivo provenga no de diversas acciones individuales del autor sino de un automatismo del sistema, sin intervención alguna del sujeto activo, puesto que variada o creada una nueva instrucción en el programa informático correspondiente, cada vez que se acceda al programa o a la base de datos, el sistema va a repetir automáticamente la manipulación²⁸⁹. (ROVIRA DEL CANTO, E. 2002:78)”

Extensa Y Elevada Lesividad

²⁸⁷ ALASTUEY DOBON: «Apuntes sobre la perspectiva...», cit., pág. 484. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 78.

²⁸⁸ Ver al respecto los supuestos objeto de enjuiciamiento por los Juzgados y Tribunales en nuestro país, recogidos en la Sección VII.1 y en el Capítulo IX, ut infra. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 78.

²⁸⁹ Por este motivo, dice SIEBER, «si se descubre una determinada manipulación del ordenador tiene que comprobarse siempre que no se hayan producido otras manipulaciones en el desarrollo del funcionamiento en su conjunto», ult. op. cit., pág. 30. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 79.

Es la segunda característica para esta clase de delitos que ha determinado el autor citado previamente, determinando que:

“Así ALASTUEY²⁹⁰ ha abordado tangencialmente la cuestión al sostener que estos hechos procuran a sus autores unas elevadas ganancias, siendo el perjuicio económico que producen muy superior al de cualquier otro tipo de conducta ilícita, incluso al causado por la delincuencia económica tradicional. Por su lado, GÓMEZ PERAL²⁹¹ alude, también desde el aspecto económico, a la «rentabilidad» de estos delitos, que calcula como «una tercera parte superior a la de cualquier otro tipo, ya se trate de una o pocas ocasiones en que se sustraen grandes cantidades o de infinidad de operaciones por un importe mínimo (técnica del salami) “, afirmando además que «la lesividad de estas acciones se acentúa porque hoy en día la interconexión entre las actividades económicas genera un efecto de «cascada» en que se ven afectadas multitud de entidades, por lo que el perjuicio aumenta considerablemente». (ROVIRA DEL CANTO, E. 2002:80)”

Dificultades De Averiguación Y Comprobación

La dificultad de su averiguación y comprobación que obedece a la necesidad de conocimientos técnicos avanzados en informática es la tercera característica que ha definido Rovira del Canto, así:

²⁹⁰ ALASTUEY DOBON: «Apuntes sobre la perspectiva...», cit., pág. 459. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 80.

²⁹¹ GÓMEZ PERAL: «Los delitos informáticos... », cit., pág. 483. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 80.

“Más que sobre la caracterización de estas peculiaridades criminológicas, se ha venido centrando la doctrina, sobre todo la española, en su análisis como vínculo causa-efecto, como base, de una de sus consecuencias, también de índole criminológica: la cifra negra u oscura, que veremos más adelante. Así se han sostenido como base de estas características el anonimato del perjuicio producido²⁹², la facilidad para encubrir el hecho²⁹³, y la disminución del riesgo de ser descubierto el autor gracias a la posibilidad de borrar todas las huellas, sin dejar rastro perceptible, una vez perpetrada su acción delictiva²⁹⁴. (ROVIRA DEL CANTO, E. 2002:82)”

Alto Volumen De Cifra Negra

Es la cuarta característica definida por el autor en cita, determinando que:

“En gran parte consecuencia de la anterior característica se desprende una elevada cifra de comportamientos informáticos delictivos que no salen a la luz, la llamada cifra negra u oscura, aunque, como ya sostenía SIEBER²⁹⁵ con métodos

²⁹² Así CAMACHO LOSA: «El delito informático», cit., pág. 69; GONZÁLEZ Rus: «Aproximación al...», cit., págs. 109 y 110 TIEDEMANN: «Poder económico y...», cit., pág. 123 Y ss. ROMEO CASABONA: «Poder informático...», cit. pág. 35; GUTIÉRREZ FRANCÉS: «Fraude informático...», cit., págs. 78 Y 79; o ALASTUEY DOBON: «Apuntes sobre la perspectiva...», cit., pág. 459. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 82.

²⁹³ DAVARA RODRÍGUEZ: «Manual de...», cit., págs. 299 y 300. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 82.

²⁹⁴ Así GUTIÉRREZ FRANCÉS: «Fraude informático...», cit., pág. 79; ROMEO CASABONA: «Poder informático...», cit., pág. 35; siguiendo a los anteriores ALASTUEY DOBON: «Apuntes sobre la perspectiva...», cit., pág. 459; Y DAVARA RODRÍGUEZ: «Manual de...», cit., pág. 300. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 82.

²⁹⁵ SIEBER: «Criminalidad informática.. », cit., pág. 32. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 87.

científicamente seguros no se puede hacer ninguna afirmación absoluta sobre cuál es el verdadero volumen de la criminalidad informática, sino tan sólo con meras estimaciones fundadas en la experiencia, pues en la inmensa mayoría de países el tratamiento de la delincuencia informática ha sido ubicado sustantiva y estadísticamente, y lo sigue siendo aunque de forma cada vez menor²⁹⁶, entre los ámbitos de delincuencia tradicional (como la económica o contra la intimidad). Incluso ROMEO CASABONA²⁹⁷ ya advertía que los estudios criminológicos al respecto no eran lo suficientemente rigurosos, siendo difícil el cuantificar dicha zona oscura; y TIEDEMANN²⁹⁸ ponía de manifiesto la imposibilidad de realizar un cálculo siquiera aproximado de la cifra negra en este ámbito. (ROVIRA DEL CANTO, E. 2002:87)”

Creciente frecuencia. Diversidad y peligrosidad

Esta es la quinta característica que el autor en cita ha establecido para los delitos informáticos y la explica de la siguiente forma:

“El conjunto de las características tradicionales anteriormente expuestas ha supuesto y supone un progresivo y creciente volumen, desarrollo y variedad de las manifestaciones de la criminalidad informática, como asimismo anteriormente hemos expuesto en apartados anteriores. Pero es que la continua

²⁹⁶ Claro ejemplo de ello se muestra en los diferentes artículos contenidos en la obra de SIEBER «Information Technology...», cit., y recogidos asimismo por la A.I.D.P. en su vol. 64, 1-2, de la «International Review of...», cit. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 87.

²⁹⁷ ROMEO CASABONA: «Poder informático...», cit., pág. 36. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 87.

²⁹⁸ TIEDEMANN: «Poder económico...», cit., pág. 123. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 87.

evolución de las nuevas técnicas, la aparición en el mercado de modems y terminales económicos y asequibles para cualquiera, «snifers»²⁹⁹, aparatos de telefonía móvil con prestaciones informáticas y telemáticas, o en los nuevos servicios a través de las vías de comunicación como Internet³⁰⁰, han confirmado las perspectivas amenazadoras de ampliación de las posibilidades de la criminalidad informática a través del teleproceso y una adaptación acelerada del delito a la tecnología de la información. Es ya una realidad el que la tecnología informática y de telecomunicación se ha extendido cerca de todas las áreas de la vida, haciéndose posibles nuevos delitos informáticos, mayor volumen de los mismos, y la afectación de más y más áreas de la sociedad. (ROVIRA DEL CANTO, E. 2002:94)”

²⁹⁹ El «sniffer» (como recoge DEL MORAL TORRES, A.: «Dificultades en la investigación de los denominados delitos informáticos», extracto del cual fue publicado bajo el título «La investigación de delitos informáticos» en la Revista «Guardia Civil», núm. 644, Diciembre de 1997, págs. 30 a 32), o rastreador «es un programa informático normalmente escrito en lenguaje de programación «C» que circula libremente en determinados foros de debate o «news» en INTERNET por lo que puede ser copiado al ordenador personal de cualquier usuario. Este programa está diseñado para ser ejecutado en una red informática y rastrear todas las transacciones que viajan por la red para volcarlas finalmente a un fichero de salida. Entre dichas transacciones pueden encontrarse palabras de paso de acceso a proveedores o números de tarjetas de crédito utilizadas para realizar operaciones bancarias que una vez contenidas en el fichero de salida pueden ser utilizadas de forma fraudulenta por el ejecutor del Sniffer», radicando su problemática en «la imposibilidad material de controlar la libre circulación a través de INTERNET de este «rasterador» así como de otros programas que pueden ser utilizados para dañar ordenadores, o manipular su información». Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 93.

³⁰⁰ Así aprovechando la existencia de páginas WEB en INTERNET que ofrecen la posibilidad de adquisición de bienes y servicios (un libro, una entrada de cine o teatro, un billete de avión, la compra de un electrodoméstico, un coche o incluso una vivienda) mediante la consignación de datos específicos de medios de pago (normalmente tarjetas de crédito), se hacen circular libremente por la red programas informáticos que generan números aleatorios de tarjetas de crédito y que son chequeados en estas páginas WEB hasta que se produce la coincidencia con algún número real, y entonces se realiza una adquisición con cargo al tercero titular de la tarjeta. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 94.

Distanciamiento Temporal Y Anulación Espacial

Esta es la sexta característica que el autor en cita ha establecido para los delitos informáticos y la explica de la siguiente forma:

“Más actualmente esta caracterización espacio/temporal de los ilícitos informáticos viene fundamentada en las propias facilidades que el tratamiento, almacenamiento, procesamiento y transferencia de la información y de los datos de los actuales sistemas informáticos y de comunicaciones llevan consigo, por un lado, de una creciente rapidez y velocidad en su realización conjuntamente a la posibilidad de interrupción, paralización o suspensión temporal en la realización completa de la acción ilícita, así como, por otro lado, en la anulación fáctica, que no desaparición física, de distanciamiento espacial entre el sujeto que realiza la acción y el lugar donde ésta materializa su ejecución y puede constatarse su realización, y no sólo en referencia a sus efectos, sino incluso en la formación de lo que se ha venido a llamar ciberespacio, ya visto con anterioridad.

Estas peculiaridades dan lugar a una eliminación, o el que se deban tener en mínima consideración, los requisitos y principios espacio/ temporales propios en la formulación dogmática de las tradicionales figuras del derecho penal, y suponen una quiebra y anulación de las reglas clásicas en materia de grados de ejecución y de las reglas competenciales procesales, pues no sólo el resultado, sino la materialización de la ejecución de la acción puede completarse infinitamente después en el tiempo, así como en un lugar o lugares distintos, lejanos físicamente de

aquél en donde se encontraba el autor, o incluso en un plano espacial virtual o irreal, lo que va a configurar otra característica más acentuada, y que veremos a continuación, de la transnacionalidad del delito informático, o, lo que es lo mismo, su carácter transfronterizo.

Y concretamente el distanciamiento temporal, en los términos ahora recogidos, da lugar a una frecuente imposibilidad material de determinar con exactitud el concreto momento de la consumación delictual efectiva al haber finalizado la acción por parte del sujeto activo sin que haya habido una efectiva materialización de resultado alguno, y quedando consecuentemente sin afectar de facto el bien jurídico tradicional que pudiera ser asimismo objeto de protección conjunta. (ROVIRA del CANTO, E. 2002:98).”

Transfronterizo

La séptima característica que el autor Español en cita ha determinado para los delitos informáticos es su categoría de transfronterizos y la define así:

“Claro ejemplo de ello es el ámbito de la difusión o distribución de contenidos ilegales o ilícitos a través de Internet, y en sus «foros de debate». Así SIEBER³⁰¹ recoge el problema que se plantea cuando las imágenes presentadas en esos foros de debate son imágenes reales de menores de edad en las cuales puede detectarse prácticas sexuales abusivas e ilegales, o incluso se ofrecen contactos con esos menores para lo cual es

³⁰¹ SIEBER: «Legal Aspects...», cit., pág. 59. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 99.

preciso abonar cierta cantidad de dinero y ponerse en contacto con el pederasta o pedófilo a través de una dirección de correo electrónico, problema que se acrecienta precisamente por la transnacionalidad de la comisión del hecho, que sucede cuando, por ejemplo, el presunto pedófilo en España «coloca» para comercializarlas las imágenes pornográficas con menores de edad en un proveedor de Internet ubicado en E.UU., donde es libre y gratuito acceder para publicar cualquier tipo de información sin que sea registrada la identidad de la persona que origina la información, y tales imágenes son captadas y recogidas por terminales y ordenadores de muy diversos países, incluso simultáneamente a través de un foro de debate. Y ante este ejemplo realmente hay que plantearse las mismas preguntas que se formula SIEBER de ¿dónde realmente se comete el delito? y ¿cómo es posible detectar el origen si no existe un registro fidedigno de quien ha colocado la información en el proveedor? Y estas consideraciones es lo que ha llevado a parte de la doctrina a apreciar la existencia de un nuevo espacio, el ciberespacio caracterizado, como ha sostenido LEVY³⁰², por una supresión de la universalidad y en una concurrencia de la totalidad. Ello, no obstante, ha llevado a propugnar desde todos los sectores la necesidad de la protección de los bienes jurídicos nacionales frente a estos delitos de forma unitaria, al menos en Europa y en los países occidentales, para evitar tergiversaciones de la competencia o para evitar un comportamiento desviado de los autores³⁰³, a proponer la construcción de un sistema europeo de

³⁰² LEVY: «Sobre la...», cit., págs 25 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

³⁰³ SIEBER, U.: «Estado de la evolución y perspectivas del Derecho Penal Económico europeo», en «Hacia un Derecho Penal Económico Europeo» (jornadas en honor del profesor Klaus Tiedemann celebradas en la Universidad Autónoma de Madrid, del 14 al 17 de octubre de 1992), Boletín Oficial del Estado, Madrid, 1995, pág. 604. Citado en: ROVIRA del CANTO,

Derecho penal implantado sobre bases homogéneas que permita una represión eficaz del ilícito transnacional³⁰⁴, o a interesar, como ya vimos en su momento³⁰⁵, una respuesta conjunta, armónica y coordinada a tales retos mediante la creación de figuras delictivas globales en un derecho penal global, o «Derecho penal de la globalización» como denomina SILVA SÁNCHEZ³⁰⁶ y en lo que considero más específico un derecho penal global del riesgo informático y de la información³⁰⁷. (ROVIRA del CANTO, E. 2002:100)».

E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

³⁰⁴ CHOCLAN MONTALVO: «Estafa por...», cit., pág. 1070. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

³⁰⁵ Ver Subsección II.3.3. ut supra. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

³⁰⁶ SILVA SÁNCHEZ, J.: «La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales», Cuadernos Civitas, Ed. Civitas, Madrid, 1999, sosteniéndolo en base a la actual expansión del Derecho penal como efecto de la que denomina delincuencia globalizada, que considera de marcado carácter económico o lucrativo (pág. 65). Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

³⁰⁷ Si bien tales predicamentos han sido expuestos desde hace tiempo, y en tal sentido SIEBER, U.: «Unificación Europea y Derecho Penal Europeo. Propuestas para el futuro del Derecho penal europeo», Estudios Doctrinales y de Jurisprudencia, Revista Colex, Año I, núm. 3, Madrid, 1992, págs. 27 y ss., lo cierto es que como recoge CHOCLAN MONTALVO, últ., op. cit., pág. 1070, hasta la fecha el único intento de construcción de un Derecho Penal europeo se ha limitado al ámbito de la protección penal y procesal de los intereses financieros de la Comunidad Europea, el titulado Corpus Iuris, entendiendo por delito transnacional al que atenta a tales intereses comunitarios de la Unión Europea. Asimismo del mismo autor: «Hacia la unificación del derecho penal comunitario. El Corpus Iuris Europeo», Diario La Ley, primera parte publicada en el número 4475, correspondiente al Lunes 9 de febrero de 1998 (AÑO: XIX), y la segunda parte en el número 4476 correspondiente al Martes 10 de febrero de 1998, pág. 3. Obtenido por acceso en dichas fechas a la página web www.laley-actualidad.es, y en el mismo sentido tanto DELMAS-MARTI, M.: «Corpus Iuris portant dispositions pénales pour la protection des intérêts financiers de l'Union européenne», versión original en francés e inglés publicado por la Direction Général du Contrôle Financier, Ed. Economica, París, 1997, pág. 10 y ss., y TEJADO LLORENTE, M.L.: «Las relaciones entre el Derecho comunitario y el Derecho Penal», Actualidad Penal núm. 3, de 19 al 25 de enero de 1998, Actualidad Editorial, Madrid, 1998, págs. 45 y ss. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 100.

El sujeto activo: el delincuente informático y su móvil.

Dentro de la adecuación de la tipicidad que realiza el autor español en cita para los delitos informáticos, ha determinado las siguientes características para los sujetos activos de estas conductas disvaliosas, así:

“RUIZ VADILLO³⁰⁸ en discrepancia de las posturas de inscribir al delincuente informático en el cuadro general del delincuente de cuello blanco de la criminalidad económica o de los negocios, sostuvo que autor del delito informático puede serlo cualquiera, no precisando el mismo de determinados requisitos personales o conocimientos técnicos cualificados, por lo que además tal consideración le llevaba a afirmar que no se constituía consecuentemente en un delito especial por este elemento.

Una extensión de la caracterización del potencial delincuente informático ya fue asumido claramente en España a finales de los ochenta y principios de los noventa; así GUTIÉRREZ FRANCÉS³⁰⁹, quien si bien se refiere a esa caracterización casi mítica del delincuente informático como adolescente de posición social media, cree que se trata de un amplio abanico que abarca desde empleados de empresas con acceso a su sistema informático, a chavales jugando con el ordenador o amas de casa. Y CHOCLAN MONTALVO³¹⁰ mantiene la consideración

³⁰⁸ RUIZ VADILLO: «Tratamiento de la delincuencia...», cit., pág. 78. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 104.

³⁰⁹ GUTIÉRREZ FRANCÉS: «Fraude informático...», cit., págs. 74 y 79. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 104.

³¹⁰ CHOCLAN MONTALVO: «Estafa por...», cit., pág. 1070. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 104.

de una categoría criminológica sui generis del delincuente informático «que se sitúa a caballo entre el delincuente de cuello blanco y aquel delincuente habitual o asocial que contempla el Derecho penal clásico, presentándose con frecuencia el delito por la acción de autores ocasionales que no precisan conocimientos informáticos especialmente cualificados, e incluso por la intervención de jóvenes que a título de mero recreo o incluso por mera curiosidad intelectual al modo de los primeros hackers (manipuladores no autorizados de sistemas informáticos) penetran en el sistema informático produciendo perjuicios de consideración».

Por su parte ALASTUEY DOBON³¹¹ sosteniendo a modo de conclusión de las posturas doctrinales anteriores, y dado que en la mayoría de las ocasiones está acreditado que el delincuente informático no posee un alto nivel socio-económico, y tal característica es esencial en el concepto de delincuencia de «cuello blanco», cree que la delincuencia informática no puede identificarse, desde un punto de vista criminológico con la reiterada delincuencia de «cuello blanco», considera que los sujetos activos «no suelen ser personas con una inteligencia superior a la media que poseen conocimientos cualificados en el campo de la informática y que por ello llevan a cabo manipulaciones sofisticadas en los sistemas informáticos, sino más bien personas con un coeficiente intelectual medio, que tienen la oportunidad de realizar el hecho y la aprovechan.

³¹¹ ALASTUEY DOBON: «Apuntes sobre la...», cit., pág. 456 y 460. Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.P. 105.

Y GÓMEZ PERALS, tras señalar los grupos sociales de posibles autores de delitos informáticos³¹², consideraba como retrato robot del delincuente informático, el de un varón, relativamente joven, profesional competente en técnica informática o bien antiguo empleado o usuario que por su trabajo o por la confianza que la empresa ha depositado en él, tiene acceso al sistema informático y conoce sus deficiencias. ROVIRA del CANTO, E. (2002:106)”

El Sujeto Pasivo: La Víctima Del Delito Informático

En el análisis doctrinal realizado por Rovira del Canto, buscando la forma correcta de realizar la adecuación típica, antijurídica y culpable de los delitos informáticos, se ha logrado la siguiente conclusión frente a quien es el sujeto pasivo de estos delitos, así:

“A raíz de los cambios de paradigmas sociales, y fundamentalmente de la incidencia y alcance de la progresiva extensión de las técnicas informáticas y de telecomunicaciones en todos los ámbitos de la vida social, y el estar su adquisición

³¹² GÓMEZ PERALS: «Los delitos informáticos...», cit., págs. 484 y 485, establecía los siguientes grupos:

«- Los operadores, programadores u otros sujetos en legítima relación con la elaboración del programa. Las personas autorizadas actúan ilícitamente cuando se extralimitan.

- Cualquier persona a través de terminales públicas o interceptando líneas de transmisión de datos a distancia, o bien causando daños a los medios informáticos, ya sean empleados descontentos o activistas con móviles políticos o ideológicos. Son terceros o extraños.

- Los titulares legítimos del sistema, por título de propiedad y por cualquier otro título que les habilite para el disfrute de dicho sistema informático». Añade que «resulta curioso cómo la utilización ilícita por los titulares suele ser medio de comisión de otros delitos como el alzamiento de bienes mediante la creación de doble contabilidad», y que «en este apartado incluiríamos la inutilización de programas por su propietario cuando se dan determinadas circunstancias». Citado en: ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares P. 105.

disponible para cualquier ciudadano medio y no sólo el poderoso estado o empresario, lo cual también ha favorecido claramente la frecuencia y la mayor diversidad de los comportamientos ilícitos informáticos como hemos visto en los apartados precedentes, en la actualidad si bien podemos seguir reconociendo que en el ámbito estrictamente económico patrimonial son las personas jurídicas en el ámbito mercantil o del comercio el objetivo principal de las acciones delictuales informáticas, que no exclusivo, a tenor de la configuración que actualmente debe darse al delito informático como delito del riesgo informático y de la información, nos lleva a afirmar que ha habido una inicial extensión de la conceptualización del potencial sujeto pasivo del mismo, pudiendo comprenderse con carácter general, no sólo a los titulares y demás beneficiarios legítimos de un sistema informático, como los usuarios y terceros de buena fe, sino incluso a cualquier persona, física o jurídica, que en cualquier momento, ocasión, o circunstancia tenga o se encuentre vinculado directa o indirectamente con un sistema informático, la información en él contenida, o los datos que la representan. (ROVIRA del CANTO, E. 2002:116).

2.6. Reflexiones Sobre la Conducta en Internet y su Influencia en la Sociedad.

Pensar en la creación de tipos penales exige un nuevo bien jurídico tutelado: la información y el dato; la discusión no podía reducirse a que son simplemente las mismas conductas ya tipificadas que se realizaban a través de otros medios.

Las legislaciones nacionales de algunos países, comenzaron a adoptar medidas legislativas siguiendo los derroteros de la CNUDMI, con la finalidad de homologar las disposiciones legislativas y con esto permitir la circulación veloz de un libre mercado digital.

No obstante, la rapidez de la inserción de las nuevas tecnologías a la sociedad, va tan rápido como la de los actores criminales, quienes descubrieron la manera de apropiarse de información, y de manera desleal, comenzaron a ejecutar una serie de prácticas atentatorias de la seguridad en la red. Este tipo de prácticas exhortaron a los Estados, que acababan de ponerse de acuerdo frente a la reglamentación del comercio electrónico, sobre la necesidad de generar acuerdos de cooperación internacional, encaminados a prevenir este tipo de conductas, así como a detener la impunidad en la comisión de estos delitos.

2.6.1. Consideraciones preliminares

El delito informático es una realidad de la sociedad informática. Su vertiginoso desarrollo y sus mutaciones constantes obedecen a múltiples y complejas condiciones. De un lado, a causa de la fragilidad en los sistemas. Los soportes y condiciones binarias del sistema son potentes y frágiles a la vez. Una máquina informática puede realizar a velocidades impensables un sinnúmero de operaciones en milésimas de segundos y a la vez fracasar por la saturación de la información y por su dependencia en la energía requerida. Los sistemas inteligentes tienen la capacidad de procesar información y a la vez se ven limitados para producir, desde unos componentes mínimos, inteligencia. Detrás de la máquina binaria está la mente humana y una de las

características de ella es la genialidad para provocar, con un mínimo de elementos, un juego infinito de aciertos.

La extensión de la mente humana es precisamente el computador; pero ella tiene sus límites. Ella busca prolongarse y a la vez encuentra sus límites. La lucha del ser humano consiste, desde la tecnología, en crear condiciones de prolongación de su inteligencia que le permitan sustituir ciertas operaciones en procesos simplificados y efectivos. Una de ellas, por ejemplo, es el cálculo y el tratamiento de una masa considerable de información. Precisamente, éste ha sido el principio generador de los sistemas computacionales, cuya función es poder reducir el tiempo, generando procesos efectivos que facilitan la información. Este proceso se ha ido modificando, perfeccionando y nutriendo de tal modo que los sistemas remplazan ciertas facultades del pensamiento. De la acumulación de información a la generación de conocimiento virtual, la especie humana se enriquece, pero también vive en otros riesgos. Por ejemplo, las formas de control de los sujetos, la constricción de la libertad, la pérdida de anonimato. Estos riesgos chocan con los valores humanos universales y ponen en el límite los intercambios. La pornografía infantil vinculada con relaciones laborales y de vida, en donde los sujetos son prisioneros de los nuevos roles y patrones de actuación, materializan un riesgo para la familia y sus tradiciones. Hoy, el gran problema de la familia consiste en tener el tiempo suficiente para compartir. Si en otros tiempos ella estaba unida por rituales en cuyo centro se encontraba la palabra, hoy ella se regula por condiciones virtuales. Así mismo, las relaciones laborales tienden cada vez a modificarse. Los sujetos y los espacios laborales se transforman progresivamente, al punto en que éstos pueden laborar en múltiples espacios y en tiempo real desde lugares diversos. La gran fábrica cede su especialidad en el ciberespacio. La empresa cada vez es más virtual, de la misma forma como la educación y la formación de un sujeto ocupan un

lugar en el ciberespacio. Las relaciones humanas, los rituales de intercambio, los procesos de socialización, las prácticas reproducción y circulación de mercancías, oferta de bienes y servicios dominan un nuevo espacio intangible. El amor se virtualiza al mismo tiempo que se deslocaliza la fábrica.

De otro lado, los procesos de intercambio en el ciberespacio tienden a consolidar nuevos patrones de cultura y a generar nuevas formas de delito. La fragilidad y la fortaleza de lo virtual y del ciberespacio se conjugan en un mismo horizonte. Por un lado, los procesos de confianza en las tecnologías de la información y de la comunicación buscan brindarle a los sujetos un sentimiento de seguridad, pero, dado que el ciberespacio es abierto y en constante movimiento, que los sistemas que delimitan dicha especialidad son frágiles y los mecanismos de control están sometidos al surgimiento de nuevas prácticas, forjando así un sentimiento de soledad. El ciberespacio, exige la fijación de unas normas con el fin de regular los intercambios y forjar principios de actuación positivos. La buena fe, el uso correcto de la información, el goce pleno de un bien, la satisfacción de una demanda requieren de normas y de principios coercitivos. El delito informático, es una manifestación de la fragilidad y de la potencia de lo tecnológico. La ecuación, curiosamente, muestra que a mayor control, mayor es la posibilidad del quiebre de dicha seguridad. Se podría decir, que una cultura del delito informático es real en su virtualidad.

Así como la velocidad es una de las características de la sociedad de la información y del conocimiento, el control una práctica de la sociedad moderna y el fraude, el robo de identidad, el saqueo o la suplantación electrónica, son las manifestaciones del delito informático. A la vez que la tecnología engendra seguridad y minimiza los riesgos en la vida diaria, los

delitos informáticos crecen de manera exponencial. Entre seguridad e inseguridad ciberespacial, se crea un espacio de tensiones. Las grandes empresas de la informática se nutren de los virus y del delito informático. La “reciprocidad” entre sujetos nunca es voluntaria, sino consecuencia de sus formas de relación. La relación entre sujetos exige confianza, para que de ella pueda surgir un compromiso humano y un ideal común. En el ciberespacio dicha confianza y solidaridad común son virtuales. Significa esto, que estos valores y principios son potencia y a la vez confianza. Así como cuando se habla de la confianza en la palabra empeñada, o como cuando se firma un contrato donde las partes confían recíprocamente, de la misma forma el ciberespacio promueve dicho sentimiento. Este espacio aunque invisible en su realidad física, existe gracias a la informática.

Por informática entendemos la transformación y transferencia de la información a través de las computadoras, cuya finalidad es realizar los procesos cotidianos de manera más eficiente. La informática también “es la disciplina que estudia el fenómeno de la información y la elaboración, transmisión y utilización de la información principalmente, aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos”³¹³, y quizá una definición más amplia “es la aplicación racional y sistemática de la información para el desarrollo económico, social político”³¹⁴. La economía del conocimiento sustenta su eje en la investigación, y su repercusión en la sociedad se concreta en múltiples hechos cotidianos y uno de ellos es el otorgamiento de derechos de patente.

³¹³ Carrion Zorzoli Hugo, “Atipicidad penal del sabotaje informático”, Revista Alfa-Redi, No. 048 – julio del 2002, <http://www.alfa-redi.org/rdi-articulo.shtml?x=1473>, ISSN 1681-5726, página consultada enero 2007. El autor participó en la redacción del Anteproyecto de Ley sobre Delitos Informáticos publicado en el Boletín Oficial 27/09/01.

³¹⁴ Altmark, Daniel Ricardo, La etapa precontractual en los contratos informáticos, Departamento de Postgrado facultad de derecho, Universidad de Buenos Aires, p. 1(documento electrónico).

Son estos derechos inmateriales o de propiedad intelectual los que actualmente precisan de una protección jurídica. Debido a su naturaleza y relevancia se convierten en derechos vulnerables y objeto de trasgresión. Precisamente “(...) el 51% de los ingresos del producto interno bruto de EE.UU. lo constituyen los derechos de patente”³¹⁵, y esto trae consigo un ejercicio complejo de salvaguarda de la propiedad. En el ciberespacio todo puede suceder, al punto que un derecho se vea vulnerado en su legitimidad.

Por todo esto, nos interesa en este capítulo dedicar un tiempo para conocer las principales formas del fraude en la contratación electrónica internacional. Nuestro objeto son los contratos, esta materia es la que precisa nuestro interés en el campo de la informática. Una definición del delito informático, a la vez que los principios de legalidad y de analogía hasta llegar a su tipicidad, nos obligan a recorrer este último momento de nuestra investigación. Al final, lograremos delimitar las reglas jurídicas para prevenir el fraude electrónico y específicamente en el ámbito internacional. .

2.7. Diferentes Conductas Relacionadas con los Delitos Informáticos

Con el propósito de tener mayor claridad frente a las conductas que constituyen en diferentes legislaciones Delitos Informáticos, debemos hacer referencia a los significados que le ha dado la doctrina jurídica a sus autores y a algunos tipos penales en particular, así:

³¹⁵ Thurow Lester, profesor de economía del MIT, citado en Delitos Informáticas ¿Robo del Siglo XXI? Trabajo dirigido por el Dr. Carlos Parma, Universidad Católica de Cuyo (San Luis), Argentina, <http://derechopenal.tripod.com/www/informaticos.pdf>, Página consultada Febrero 2007

Hacker

Hacker es una palabra que deriva del vocablo hack traducida como corte, hachazo, tajo, puntapié, mella. “La definición más comúnmente asociada al término hacking hoy día es intrusión sigilosa en un sistema informático sin autorización”³¹⁶. Con la expresión hacking, se hace referencia a un conjunto de comportamientos de acceso o interferencia subrepticios, a un sistema informático o red de comunicación electrónica de datos y a su utilización, sin autorización o más allá de lo debido³¹⁷. De esta manera podemos ubicar a dicha figura como un accionar diferenciado a cualquier otro, en donde sólo se busca ingresar ilegítimamente a sistemas de información, sin la intención de dañar o

³¹⁶ Crimen y castigo en el ciberespacio Disponible en <http://skyscraper.fortunecity.com/graphical/472/crimen.html#VII>. Y según otros expertos, la palabra deriva de *hack*, un término que se usaba para describir la familiar forma en que los técnicos telefónicos arreglaban cajas defectuosas; el viejo pero efectivo golpe seco. La persona que realizaba esa operación era, naturalmente, un hacker. Independientemente de la raíz etimológica de la palabra, lo que sí parece objeto de consenso es que serían los estudiantes del famoso MIT (Massachusetts Institute of Technology) los que acercaran la acepción del término a una definición en la que se incluían ordenadores. Efectivamente, ya en 1959 algunos estudiantes se reunían a través de un ordenador IBM 407. Por aquel entonces, era común que el ordenador fallase por razones extrañas y las reparaciones consistían a veces en aplicar un buen golpe en el costado del ordenador: un método de sorprendente eficacia para la tecnología a base de válvulas de la época. Según la definición de The New Hackers Dictionary de Eric Raymond, “*los hackers son inteligentes, intensos, abstraídos e intelectualmente abiertos. Se interesan por cualquier sujeto que les pueda proporcionar estimulación mental y es común que tengan una afición extrema al hacking, en el que se desenvuelven competentemente. Les encanta el control, pero no en forma autoritaria sino sobre cosas complicadas, como las computadoras. Se apasionan por lograr que esas máquinas sean instrumentos de lo interesante, siempre y cuando se trate de sus propias ideas y no de una orden de alguien. No les gustan las rutinarias tareas cotidianas que llevan a mantener una existencia normal; por ello, si bien son ordenados en sus vidas intelectuales, son caóticos en el resto. Prefieren el desafío del conocimiento a una recompensa monetaria por un trabajo*”. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 97.

³¹⁷ SÁEZ CAPEL, José, informática y delito, Proa XXI Editores, 1ª ed., Bs. As., 1999, p. 87. Empero tal delimitación resulta insuficiente, pues el acceso no autorizado puede deberse a diversas motivaciones: puede ser un simple juego o respuesta al reto permanente que la máquina significa para el hombre, pero también en ocasiones se presenta como modus operandi de un ilícito más grave, tales como fraude, sabotaje, etc. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 98.

*alterar los sistemas, afectando solamente la confidencialidad y exclusividad de la información*³¹⁸.

*Esta denominación que denota una serie de conductas que específicamente hacen referencia al acceso no autorizado propiamente dicho a sistemas informáticos ajenos, presupone que se han burlando las medidas de seguridad (contraseñas, claves de acceso, etc.) dispuestas para impedirlo y que ponen de manifiesto la voluntad del titular de que sólo las personas autorizadas por él puedan utilizar los recursos o ficheros informáticos, o tengan acceso a la información que se contiene en ellos. La actividad del hacker en un sistema puede tener distintas finalidades, pero por lo general, en la mayoría de los casos, sólo tiende a eliminar los pasos de seguridad del sistema con el solo objeto de ver el contenido de la información protegida. Refieren los autores a una subcultura del hacker (hackerdown), compuesta por personas particularmente creadoras, con un vocabulario particular, utilizado como todo argot como herramienta de comunicación, a la vez que como exclusión o inclusión. Estos grupos se encuentran organizados conforme a un sistema de valores, normas y conductas compartidas*³¹⁹. CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009:101)

³¹⁸ HOCSMAN, Heriberto Simón, "Delitos informáticos", Simposio Argentino de Informática y Derecho, 2003. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 98.

³¹⁹ SÁEZ CAPEL, José, ob. cit., Ps. 89 y 92. Según la tradición oral, esta pasión por el intrusismo tuvo sus inicios con la película de John Badman, Juegos de guerra, en la que el protagonista es un joven que estuvo casi a punto de desatar la tercera guerra mundial, al haberse introducido en el sistema computado de defensa de los Estados Unidos. Por cierto, una ficción. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 98.

Cracker

Para las acciones nocivas existe la más contundente expresión, cracker o “rompedor”. Sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender. Es decir, presenta dos vertientes, el que se infiltra en un sistema informático y roba información o produce destrozos en él, y el que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia. El cracker tiene como intención destruir³²⁰. CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009:101)

Virucker

La denominación referida proviene del apócope de las palabras virus y hacker, definiendo de esta manera a aquella persona que “programa virus informáticos que se insertan dolosamente en sistemas informáticos, siendo una variante precisamente el que inserta un programa contaminado sin haber intervenido en el diseño del programa destructor”³²¹. Dicho accionar consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir “virus” y destruir, alterar y/o inutilizar la información contenida.

³²⁰ Disponible en <http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 100.

³²¹ FILLIA, Leonardo César; MONTELEONE, Romna; NAGER, Horacio Santiago, SUEIRO, Carlos Christian, Análisis integrado de la criminalidad informática, Fabián J. Di Placido Editor, Bs. As., 2007. En cita a Marcelo Alfredo RIQUERT, p. 120. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 101.

*Existen dos tipos de virus (tratados anteriormente), los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores*³²². CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009:101)

Phisher

*Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser información detallada sobre tarjetas de crédito, una contraseña u otra información bancaria. Quien lo practica es conocido con el nombre de phisher. El término phishing viene del inglés fishing que significa pesca, haciendo alusión al acto de pescar usuarios mediante carnadas o señuelos fabricados por los phisher cada vez más sofisticados y de este modo obtener información financiera y contraseñas. También se dice que el término phishing es la contracción de password harvesting fishing que significa: cosecha y pesca de contraseñas, aunque esto probablemente es un acrónimo retroactivo*³²³. CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009:102)

³²² Disponible en <http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 102.

³²³ Disponible en <http://www.descargar-antivirus-gratis.com/phishing.php>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 102.

3. LEGISLACIÓN FRENTE A LOS DELITOS INFORMÁTICOS, ELECTRÓNICOS Y DE LAS TELECOMUNICACIONES EN LA CIBERSOCIEDAD.

3.1. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en la Unión Europea.

Los diferentes países de la Unión Europea han realizado significativos avances en lo referente a la regulación legal penal de los injustos sociales que atenten contra los Datos y telecomunicaciones, realizados a través de medios informáticos.

Alemania y Francia son las naciones cuya legislación en materia informática ha logrado mayores resultados, iniciando este recorrido legislativo desde mediados de la década de 1980, así:

➤ Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica, a través de la cual se reforma el Código Penal (art. 148 del 22 de diciembre de 1987) con la finalidad de tipificar unos nuevos delitos:

- Espionaje de datos (202a)
- Estafa informática (263a)
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el

engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273)

- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- En cuanto la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.³²⁴ (RINCÓN RÍOS, J. 2013)

➤ Francia

La primera iniciativa legislativa en tratar la materia data de finales de la década del 80, la Ley 88/19 del 5 de enero de 1988 sobre fraude informático. Resulta importante destacar que este país contempló la necesidad de incluir en su Código Penal un capítulo que regulara de manera específica lo concerniente al delito informático. Entre los aspectos más importantes se pueden enunciar los siguientes:

³²⁴ Seguridad de la información, *Delitos Informáticos-Legislación Alemania*, www.segu-info.com.ar, última actualización 21/08/05, página web consultada en febrero de 2007. Citado en: RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de tesis doctorales No. 13. Bogotá: Grupo Editorial Gustavo Ibáñez.

- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro³²⁵.

De manera más reciente encontramos la aplicación de la nueva tendencia en la regulación de internet, *la autorregulación*, la cual, como veíamos en párrafos anteriores, obedece a uno de los dos grandes paradigmas a través de los cuales se postulan las diversas tendencias sobre la manera de reglamentar las actividades realizadas a través de la red. Es así como se presentó un primer Proyecto de Estatuto el 5 de marzo de 1997 sobre la Utilización de Internet (*Charte de l'Internet*), a cargo del Grupo de trabajo del Ministerio de Correos y Telecomunicaciones.

Siguiendo la tendencia del mecanismo de la *autorregulación*, la finalidad del estatuto es evitar litigios y propiciar soluciones rápidas y efectivas a las reclamaciones de los consumidores inconformes. “En el marco de dicho

³²⁵ Seguridad de la información, “Delitos Informáticos-Legislación Francia”, www.segu-info.como.ar, última actualización 21/08/05, página web consultada en febrero de 2007. Citado en: RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

estatuto, se ha elaborado un código de conducta sobre la utilización de Internet que contiene las definiciones de los diversos agentes (suministradores de infraestructura, servicios, acceso y contenido). Además, en él se define su ámbito de aplicación y se declara la importancia de los principios de dignidad humana; protección de los menores, la ley y el orden; protección de los derechos y libertades fundamentales; protección de los derechos de propiedad intelectual; y protección de los consumidores.”³²⁶ (RINCÓN RÍOS, J. 2013)

3.2. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Estados Unidos.

En Estados Unidos de Norte América, el desarrollo legal para minimizar las lesiones a través de delitos Informáticos inició a la par de las grandes naciones Europeas a partir de 1984 regulando a través de Actos y leyes Federales las conductas sociales informáticas capaces de causar daños a la población, la seguridad o los sistemas, así:

- Electronic Signature in Global and National Commerce Act
- Computer Fraud and Abuse Act (1984)
- Ley Federal de Protección de Sistemas (1985)
- Ley Federal sobre Fraude Mediante Transmisiones por Cable.
- Electronic Communications Privacy Act (1986)
- Small Bussines Computer Security and Education Act
- Acta Federal contra el abuso Computacional, (1994, 18 U.S.C Sec. 1030)
- Economic Espionage Act de 1996

³²⁶ Fernández de Soto, María Clara, op. cit., p. 174 -175. Citado en: RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

- Anticounterfeiting Consumer Protec, 1996
- Criminal Copyright Infringement Statute, 1996
- Modificadopor la Non Electronic Theft Act
- National Stolen Property Act. (RINCÓN RÍOS, J. 2013)

3.3. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Canadá.

La legislación canadiense no se ha quedado atrás frente a los desarrollos legislativos Europeos y de Estados Unidos, desde 1982 se promulga la Ley de acceso a los documentos de los Organismos Públicos y de protección de datos personales, dando inicio al avance legal que permite la protección de los bienes jurídicos individuales y colectivos, así:

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Quebec 1982.*

Ley de acceso a los documentos de los Organismos Públicos y de protección de datos personales de 12 junio 1982 de Quebec, modificada en 1 de marzo de 1987.

- Ley de acceso a la información y de protección de datos personales de 7 de Julio de 1982 de Canadá.
- Adhesión en 1984 a las Guidelines on the Protection of Privacy and Transborder Flows of Personal Data de 1980.
- Criminal Law Amendment Act de 20 de junio de 1985.
- Ley de la Provincia de *Ontario* de 1987.
- The Privacy Act, 1991. Privacy Commissioner of Canadá. *Ottawa*.
- Loi sur la protection des renseignements personnels dans le secteur privé (sanctionné le 15 juin 1993).

- The Uniform Electronic Evidence Act. Adopted by the Uniform Law Conference of Canada in August 1998.
- The Uniform Electronic Commerce Act. Adopted by the Uniform Law Conference of Canada on September 30, 1999.
- Land Title Amendment Act, 1999, Bill 93 *British Columbia*.
- Electronic Information, Documents and Payments, Bill 70, 2000. *Ontario Province*.
- Loi sur la protection des renseignements personnels et les documents électroniques
- Loi qui a obtenu la Sanction royale le 13 avril 2000. Personal Information Protection and Electronic Documents Act (Bill C-6). (in force on May 1, 2000).
- Red Tape Reduction Act 1999. *Ontario* (in force on June 30, 2000).
- The Electronic Commerce Act 2000 (ECA). *Ontario*. (in force on October 16, 2000).
- The Electronic Commerce and Information Act. *Manitoba* (in force on October 23, 2000).
- Personal Information and Electronic Documents Act.
- Electronic Information and Documents Act, Bill 38 *Saskatchewan Province*. (in force on November 1, 2000).
- The Electronic Commerce Act. *Nova Scotia*. (in force on December 1, 2000).
- The Electronic Commerce Act. 2000. *Yukon*.
- DORS/2001-6 - 13 décembre 2000. Règlement précisant les organismes d'enquête. Ministère de l'Industrie.
- DORS/2001-7 - 13 décembre 2000. Règlement précisant les renseignements auxquels le public a accès. Ministère de l'Industrie.
- DORS/2001-8 - 13 décembre 2000. Décret liant certains mandataires de Sa Majesté pour l'application de la partie 1 de la Loi sur la protection des

renseignements personnels et les documents électroniques. Ministère de l'Industrie.

- DORS/2001-6 - 13 décembre 2000. Règlement précisant les organismes d'enquête.
- The Electronic Transactions Act. Bill 13. *British Columbia*. (April 5, 2001)
- Loi sur les renseignements médicaux En vigueur depuis le 25 avril 2001.
- Loi sur la protection des renseignements personnels dans le secteur privé de la *province de Québec* 11 décembre 2003.

3.4. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Iberoamérica.

3.4.1. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en España.

3.4.1.1. Delitos vinculados a la informática en el Derecho Penal Español.

3.4.1.1.1. Delincuencia vinculada a las tecnologías de la información y la comunicación

Las nuevas tecnologías han creado conductas novedosas objeto de regulación legal por parte de los Estados, en palabras de De la Mata Barranco y Hernández Díaz, cuando se habla de tecnologías de la información y comunicación (TIC's) y conductas atentativas contra las mismas, en el intento por precisar los diferentes prismas desde los que puede enfocarse su tratamiento como delitos informáticos, han sido numerosas las clasificaciones

que se han efectuado de ellas³²⁷, que, fundamentalmente, se dirigen a distinguir, en relación a agresiones tanto de carácter interno como externo, esto es, tanto desde dentro como desde fuera del ámbito de utilización autorizada del sistema, ya se dirijan las mismas contra intereses del gestor del sistema ya contra intereses ajenos, ya en su comisión por el propio usuario, ya contra él. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:159-160)

En el intento de realizar una clasificación eficaz, la doctrina Española ha diferenciado cuatro grupos de criminalidad informática, el primero referido a aquella cuyo sujeto pasivo son los sistemas informáticos en sí mismos, el segundo grupo, aquel en el que la actuación lesiva recae sobre los datos, el tercero es aquel grupo en el que los sistemas informáticos se utilizan como medio para la comisión de las conductas punibles, y el cuarto y último grupo es aquel en el que se enmarcan las conductas que atentan contra los derechos digitales e informáticos.

De la Matta BARRANCO y Hernández Díaz, autores españoles, han definido estos cuatro grupos de la siguiente forma:

“1º) El que abarca lo que es la delincuencia que tiene por objeto el ataque a los sistemas informáticos en sí mismos considerados, con repercusión o no en el desarrollo de la actividad que permiten los mismos.

2º) El que se refiere a la delincuencia que tiene por objeto los datos con los que se trabaja informáticamente, ya tengan carácter personal, ya carácter empresarial, desarrollada mediante la utilización de contextos

³²⁷Sobre distintos intentos de clasificación, GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pgs. 62 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 159. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

digitales, que es al que en sentido más estricto se reserva por algún autor la caracterización de Derecho penal informático por tratarse de agresiones contra y a través de sistemas informáticos. Como a menudo se señala, en realidad el resto de grupos no abarcan sino delitos tradicionales cometidos contra nuevos objetos materiales o a través de nuevas modalidades de conducta nucleados unos y otras en torno al hecho informático o cibernético.

3º) El que engloba todas las conductas que se sirven de los sistemas informáticos para facilitar la actuación delictiva, ya sea de un tercero contra el titular o el beneficiario del sistema, ya sea de éste contra un tercero, que favorecen nuevas formas de ataque a bienes tradicionales o que al menos facilitan la extensión de la lesividad, la peligrosidad o la proliferación de los ataques a tales bienes.

4º) Finalmente, el que comprende lo que es la delincuencia que pretende únicamente atentar contra los derechos derivados de los procesos de innovación informática o de gestión de determinados derechos digitales. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:160)”

3.4.1.1.1.1. Delitos cometidos contra sistemas informáticos

3.4.1.1.1.1.1. Delitos de Daños (atentados contra la integridad de los sistemas y los datos)

De la Matta Barranco y Hernandez Díaz, citando a González Rus, han establecido que *La legislación y doctrina Españolas han desarrollado una*

subclasificación de los delitos informáticos, electrónicos y de las telecomunicaciones, teniendo como primer grupo de estudio, el de los delitos de Daños, donde encontramos, una serie de conductas vinculadas con los sistemas informáticos que entrarían dentro de los delitos de daños, concebidos éstos como destrucción, deterioro, alteración, inutilización o menoscabo de una cosa; estos delitos permiten sancionar tanto los daños que afecten a los sistemas informáticos en cuanto a los elementos materiales que incorporan (hardware) -art. 263- como los que afecten a los datos, programas o documentos contenidos en dichos sistemas, redes o simples soportes informáticos, que la doctrina viene denominando elementos lógicos (software) -art. 264.2-, también denominados conductas de sabotaje informático³²⁸, cuando tengan carácter doloso y, en el primer caso, superen los cuatrocientos euros (si no, habrá que acudir a la falta del art. 625), debiendo remitir la conducta al art. 267 pfo.2 en caso de daños imprudentes; conductas, como se ha destacado reiteradamente, en principio sin ánimo de lucro³²⁹. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 161)

En este primer grupo, Delitos de Daños, según los autores en cita, estos abarcan *-en lo que la delincuencia informática tiene de específico, al margen de la mera destrucción de los equipos informáticos equiparable a la de cualquier otro tipo de bien inventariable o del material informático que pueda*

³²⁸Véanse GONZÁLEZ Rus, «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 Cp)», pg. 1281; del mismo autor, «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», pg. 248, entendiendo que en los daños informáticos estarían incluidos tanto los daños a elementos físicos como los daños a elementos lógicos de los sistemas; en contra, MATA Y MARTÍN, *Delincuencia informática v derecho penal*, pg. 59, considera dentro de los sabotajes informáticos sólo los ataques a los elementos lógicos del sistema o aquellos que, por afectar a los elementos físicos, dañan también aquéllos. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 161. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³²⁹Por todos, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet*, pgs. 110 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 161. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

considerarse de carácter fungible- todo tipo de conducta de sabotaje informático desarrollada mediante instalaciones de bombas lógicas, gusanos, programas maliciosos, troyanos, o virus (cualquiera dentro de la tipología que abarca el concepto de cracking o «vandalismo informático»³³⁰); conductas que afectan, además de al valor del equipo dañado en sí en cuanto a la estructura y funcionamiento de sus elementos lógicos, también a la integridad de la información en él contenida, ya sea mediante el borrado irreversible de información almacenada, ya, por ejemplo, mediante la alteración o corrupción de la programación favoreciendo la causación de errores aleatorios en el funcionamiento del sistema³³¹. Es cierto, no obstante, que la magnitud del daño causado o la potencialidad para causarlo puede ser muy diferente dependiendo del tipo de ataque y ello debiera tenerse en cuenta a la hora de prever la pena correspondiente³³². (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 162) Quiere decir lo anterior, que para la Dogmática penal Española, los delitos informáticos de daños implican los resultados lesivos tanto a la información contenida, como a los equipos que la contienen cuando cumpliendo con los componentes de modo del tipo penal estos equipos ven afectada su función y actividad lógica.

Frente a la tasación de la pena, Llama la atención la mayor penalidad, en el Código penal español, de la afección al software frente a la del hardware cuando la conducta es dolosa. A este respecto hay que señalar que, siguiendo el mandato del Convenio sobre cibercriminalidad y la descripción que del

³³⁰ Utiliza el concepto de *ciberpunking* en el mismo sentido, MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pgs. 41 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 162. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

³³¹ Véase entre otros, Gutiérrez Francés, "Delincuencia Económica e informática en el nuevo Código Penal". Pgs. 291 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 162. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

³³² A este respecto, por todos, Choclán Montalvo, "Infracciones patrimoniales en los procesos de transferencia de datos". Pg. 92. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 162. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

delito de «atentado contra la integridad de los datos» se realiza en su art. 4, donde se exige sancionar como infracción penal la conducta de «dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos», y el correspondiente art. 4 de la Decisión Marco de 2005, el Proyecto de Reforma del Código Penal de 2009 desplaza el contenido del art. 264.1 al texto del art. 263 en un nuevo apartado segundo que mantiene la pena agravada y convierte el art. 264.2 vigente en un nuevo art. 264, totalmente autónomo, que sanciona, pero ahora ya con prisión de seis meses a dos años -inferior a la del tipo agravado aunque todavía superior a la del básico- a quien «sin autorización y de manera grave borre, dañe, deteriore, altere, suprima o haga inaccesibles datos o programas informáticos ajenos», y con pena de seis meses a tres años -no se entiende por qué debe ser mayor aquí la pena- a quien también sin autorización y de manera grave «obstaculice o interrumpa el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo, o haciendo inaccesibles datos informáticos». Téngase en cuenta que, a pesar de la aparente mayor amplitud de las conductas descritas, las mismas ya se venían interpretando podían formar parte de los conceptos de daño, alteración o inutilización del actual art. 264.2 -con dudas, sin embargo, en cuanto a la obstaculización o interrupción-, con lo que la nueva previsión, quizás frente a la intención inicial, lo que conlleva es simplemente un menor rigor punitivo, tanto por la exigencia de que el daño causado sea «grave» -que dificulta, además, interpretar si en los casos de ausencia de tal gravedad, superando o no el daño los 400 euros, podrá acudir al art. 625, si el concepto de gravedad debe equipararse al daño de más de 400 euros, opción que puede considerarse lógica, pero que es difícil de atender en los supuestos de obstaculización o interrupción, en cuanto estamos ante un daño que excede el que sufre el objeto material del delito, algo que tradicionalmente siempre se ha exigido, o si tal exigencia destipifica de facto, respecto a ese tipo de daños en software, los supuestos que pudieran en otro caso ser

considerados como falta-como por la referida reducción de la pena. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 162)

Vemos entonces que los delitos de daños que se encuentran dentro del grupo de delitos contra los sistemas informáticos, hacen parte fundamental del desarrollo legal Español en materia de ciberdelincuencia. Este tipo de delitos pueden diferenciarse de los otros grupos teniendo en cuenta el objeto material sobre el que recae la acción punible, pues lo son los equipos y datos informáticos, lo que quiere decir, que este objeto material puede ser tanto tangible como intangible, sin embargo, cuando la conducta recae sobre objetos materiales de tipo intangible, como lo son el software, los datos y la información contenida en los equipos, la conducta punible será agravada en cuanto a la tasación de la pena y esta condición se debe a la dificultad de recuperación de los datos, software e informaciones, puesto que son irremplazables en caso de pérdida.

3.4.1.1.1.2. Delitos de hurto y apropiación indebida y delitos de robo

En la legislación Española, el delito o la falta de hurto consiste simplemente en el apoderamiento de una cosa mueble ajena. En el contexto de la securización digital esta figura puede entrar en juego, y de ahí la necesidad al menos de su consideración, al margen por supuesto de apoderamientos de material informático, de la clase que sea, que no revisten particularidad alguna en relación con el apoderamiento de cualquier otro tipo de bien³³³, en relación

³³³Véase, por todos, GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», pg. 117 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 166. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

a supuestos de incorporación al ámbito de dominio patrimonial de un sujeto de objetos ajenos que permitan el acceso a lugares, recintos, informaciones, documentaciones, etc., sin autorización. La sustracción de tarjetas magnéticas con incorporación de información digitalizada será el supuesto habitual. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 166)

Quiere decir lo anterior, que dejando de lado el tipo de bien y objeto material de la apropiación, el hurto se configura sacando un bien mueble del ámbito de dominio del poseedor, pero además, se necesita un elemento de configuración en la tipificación y es que este bien mueble genere acceso a lugares, informaciones, documentaciones o datos para que tenga la clasificación de delito informático. Este es el caso concreto de las tarjetas magnéticas.

Así lo han establecido De La Matta Barranco y Hernández Díz, cuando dicen que *en caso de que el objeto -la tarjeta- ya la tenga en su poder el sujeto en cuestión, tras haberla recibido lícitamente, su apropiación definitiva habiendo finalizado ya el período de autorización para su utilización -por ejemplo, por haber cesado en el puesto de trabajo-, dará lugar al delito o la falta de apropiación indebida. La misma infracción habrá que aplicar cuando se trate de un objeto perdido o de dueño desconocido.* (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 166)

En relación a ambas tipologías delictivas, han de resaltarse simplemente tres cuestiones. La primera, que sólo cabe una u otra infracción, con los conceptos hasta ahora utilizados de hurto o apropiación indebida, respecto de objetos corporales, no respecto de informaciones, fluidos o energías. Sólo cabe apoderamiento -hurto- o apropiación -apropiación indebida-, además, de

cosas susceptibles de desplazamiento físico; y que sean, claro está, ajenas. No cabe, y aunque sea obvio el señalarlo, hurto de identidad digital, hurto de información digitalizada o apropiación indebida de conocimientos de acceso a sistemas de securización digital³³⁴. Las conductas que se encuadran en el Convenio de Budapest dentro del art. 6 dedicado al «Abuso de equipos e instrumentos técnicos» en relación con la obtención «de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático» (art. 6.1.a.2.), quedan fuera de lo que tradicionalmente se ha recogido en el hurto y la apropiación indebida; serían, en su caso, actos preparatorios del delito que se vaya a cometer a partir de dicha obtención; otra cosa es la obtención «de un dispositivo, incluido un programa informático» (art. 6.1.a. 1.) con soporte material. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 167)

La conducta delictiva enmarcada en el artículo 6 del Convenio de Budapest (Abuso de dispositivos) queda por fuera de la protección de bienes jurídicos tutelados consagrada en la legislación penal española, puesto que no hay una tipificación que permita darle tratamiento exacto a las siguientes conductas:

“Artículo 6. Abuso de los dispositivos.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

³³⁴Comenta CHOCLÁN MONTALVO, «Fraude informático y estafa por computación», pgs. 319 y ss.; 351 y ss., la posibilidad de considerar la apropiación de información ajena contenida en un ordenador como delito o falta de hurto, lo que, lógicamente además, difícilmente es viable en ordenamientos como el español. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 166. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Cualquier conducta que configure lo establecido en este artículo tiene la característica de ser acto preparatorio de otro delito, o ser un elemento normativo que permita la configuración de otro tipo penal.

Los autores españoles previamente citados fijan una segunda posición frente a las tipologías delictivas, y es aquella *en que la distinción entre delito y falta viene marcada por el valor corporal del objeto sustraído o apropiado; con independencia del beneficio o del perjuicio patrimonial que puedan obtenerse o causarse; y con independencia de que la utilización posterior de ese objeto que da acceso a un lugar o a una información conduzca a una actuación de carácter delictivo, en cuyo caso habrá de aplicarse además la pena que corresponda a la nueva infracción cometida en caso de que ésta exista efectivamente, sea cual sea, en el ámbito patrimonial o de tutela de la intimidad, por ejemplo.* (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 167)

Así mismo continúan los citados con un tercer punto de análisis frente a estos tipos penales, definiendo la tercera cuestión metodológica así: *a nuestro entender el uso temporal de sistemas informáticos o soportes digitales es, en sí mismo considerado, también irrelevante penalmente desde el punto de vista de los delitos de apoderamiento³³⁵, sin que puedan entenderse ubicables en este contexto los supuestos de acceso ilícito o de abuso de equipos o instrumentos informáticos a que alude el Convenio de Budapest, al menos tal y como se vienen configurando dogmática y legalmente los tipos de hurto y apropiación indebida.*

³³⁵De nuevo, GONZÁLEZ RUS, «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», pgs. 119 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 167. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

Ahora, en comparación con el delito de hurto agravado y calificado –para el caso Colombiano- tenemos que la Legislación Española *en cuanto al delito de robo con fuerza en las cosas (hurto agravado en muchas legislaciones) -el de robo con violencia o intimidación sería similar a estos efectos, excepto en relación con el dato añadido al apoderamiento patrimonial- implica también una sustracción, como en el caso del hurto, pero utilizando medios comisivos concretos -los descritos en el art. 238 del Código-, especialmente desvalorados*³³⁶. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 167)

Es en este momento interpretativo donde los autores españoles nos enseñan cómo cada una de estas conductas debe analizarse desde el principio penal de Acto, encontrando grandes diferencias entre los delitos de contenido patrimonial y económico, así:

Se trae a este contexto únicamente para recordar, en primer lugar, que el robo puede utilizarse para apoderarse patrimonialmente del objeto que incorpore la información que permite el acceso a un sistema -una tarjeta magnética-, en cuyo caso la conducta siempre implicará la comisión de un delito, con independencia del valor del objeto sustraído, al menos en ordenamientos como el español, sea cual sea el valor que se asigne al objeto.

En segundo lugar, téngase en cuenta que habiéndose obtenido mediante un delito de hurto o de apropiación indebida un objeto que incorpore información de seguridad digital -la tarjeta de identificación referida-, la misma puede utilizarse para la comisión de una infracción patrimonial, en cuyo caso podríamos estar en el ámbito de aplicación

³³⁶Igualmente, GONZÁLEZ RUS, ob. cit., pgs. 122 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 167. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

del delito de robo, considerada la tarjeta magnética como una llave y en función de lo que prescriben los artículos 238.4º y 239 pfo. 2º. En el caso de que el posible apoderamiento patrimonial surja tras la quiebra de mecanismos de seguridad específicos estaremos igualmente en el ámbito del delito de robo, en función, en este caso, de lo que prescribe el art. 238.5º. Siempre, y hay que insistir en ello, que a la utilización de la tarjeta siga -o se persiga- el apoderamiento patrimonial. No en otro caso, que nos obligaría a quedarnos únicamente con el hecho de la sustracción o apropiación de la tarjeta en sí o, en su caso, a acudir al ámbito de tutela de la intimidad, por ejemplo, en el caso de que lo que se persiga sea el acceso a una información no autorizada.

En tercer lugar, que sigue vigente, y a ello se aludirá posteriormente, la discusión sobre el tratamiento de incorporaciones patrimoniales mediante tarjetas que no permiten, sin clave de identificación, acceso a los activos ajenos.

Finalmente, obsérvese que en este contexto se entienden los delitos patrimoniales como delitos contra los sistemas informáticos en cuanto al valor que tienen estos en sí, con independencia de que también los delitos patrimoniales entren en juego cuando haya que calificar las defraudaciones patrimoniales cometidas mediante sistemas informáticos. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 168)

3.4.1.1.1.3. Delitos de defraudación (Abuso, acceso, utilización fraudulenta de equipos informáticos)

Acerca de los delitos de estafa y otras defraudaciones en relación con la utilización de sistemas informáticos para obtener ventajas patrimoniales, citando a Fernández Teruelo, tenemos que *en este grupo de delitos hay que aludir a los supuestos en los que lo que se pretende es la obtención de un beneficio derivado directamente de la utilización abusiva de un sistema digital, lo que en el Convenio de Budapest se denomina «acceso ilícito a sistemas informáticos» (art. 2) y, en su caso, «abuso de equipos o instrumentos informáticos» (art. 6), cuando el mismo tenga por finalidad dicho acceso, con independencia de que la utilización del sistema se realice en la ubicación física del equipo informático o no, pues puede utilizarse el terminal a distancia, por ejemplo, mediante troyanos que se hacen con el control del ordenador.*

Quiere decir el autor, que en la conducta delictiva de Defraudación, existe un componente subjetivo dentro del tipo penal, condicionando la configuración delictiva al propósito de obtener un beneficio derivado de la defraudación, es así, como sin este requisito subjetivo no podría configurarse este delito.

“Entre estas conductas habría que hacer referencia al denominado intrusismo informático en su versión de hacker blanco, que accede o interfiere de modo no autorizado en un sistema informático o red de comunicaciones electrónica de datos, utilizando los mismos sin autorización o más allá de ella o que simplemente penetra en los sistemas informáticos por el placer de superar las barreras de seguridad, quizás mejor ubicadas en el siguiente gran grupo de delitos. Asimismo, los supuestos de acceso a los servicios que pueda permitir el terminal. Utilizando la terminología al uso, en ocasiones se alude a

conductas de phreaking (utilización fraudulenta de conexiones de voz, imagen o datos, que permite al autor de la misma no tener que afrontar su coste) o de wardriving (variante de la primera y que supone la conexión fraudulenta a un sistema de conexión inalámbrico ajeno)³³⁷. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 169)

En el Código penal español es el art. 256 el que contempla la utilización no autorizada de un terminal de telecomunicación. En él, no es necesaria una utilización en la ubicación física del equipo informático, pues puede utilizarse el terminal a distancia, por ejemplo, mediante troyanos que se hacen con el control del ordenador. Ahora bien, téngase en cuenta que, por una parte, no es típico el mero uso indebido del terminal si de él, en sí mismo considerado, no se deriva perjuicio alguno, de más o menos de 400 euros -por lo que de nuevo aquí el denominado intrusismo informático en su versión de hacker blanco, que accede o interfiere de modo no autorizado en un sistema informático o red de comunicaciones electrónica de datos, utilizando los mismos sin autorización o más allá de ella o que simplemente penetra en los sistemas informáticos por el placer de superar las barreras de seguridad, sin causación de perjuicio patrimonial alguno, tampoco puede subsumirse en este precepto-, y que, por otra, tampoco es típico el acceso a los servicios que pueda permitir el terminal si tampoco de ello se deriva tal perjuicio.

Tal como está redactado, sólo sanciona las conductas de utilización que generan un perjuicio patrimonial al titular legítimo del servicio que tiene que abonar un coste mayor o menor por dicha utilización no consentida, ya sea, por ejemplo, porque se produce una utilización de

³³⁷Más detenidamente, FERNÁNDEZ TERUELO, *Ciberdelitos*. Los delitos cometidos a través de Internet, pg. 152. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 169. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

un teléfono de pago para acceder a redes informáticas, ya porque en sistemas de tarifa plana se produce un acceso a bases de datos u otros servicios por los que ha de pagar el titular; pero ni se penaliza el enriquecimiento del usuario ilícito (mera utilización temporal no consentida de un terminal de comunicación), ni la privación de la posibilidad de obtener un beneficio por la prestación de un servicio que no se contrata al disfrutarse de él gratuitamente (captación de señales de un router inalámbrico que evita altas en sistemas de banda ancha, aunque disminuya la capacidad del sistema que se interfiere), sino sólo el perjuicio del titular del terminal por el costo que le ocasiona la intervención ajena.

En todo caso, es cierto, como ya antes se señalaba, que cada vez se configura más como delito básico de carácter informático la mera utilización ilícita de un terminal de comunicación, el simple acceso ilegal al mismo. Dicha normativa, que prescinde del aspecto patrimonial, encuentra mejor acomodo, sin embargo, en el ámbito de la tutela de la privacidad o la intimidad -o quizás mejor en el de la tutela de lo que se entiende por libertad o seguridad informática-, como parece entender en parte el Proyecto de 2009 con el nuevo art. 197.3, vinculado no obstante a la tutela de la intimidad, ya se plantee sin ningún requisito adicional, ya exigiendo, por ejemplo, la vulneración de algún tipo de medida de seguridad diseñada ex profeso; la exigencia de alguna intencionalidad añadida obligaría a ubicar el precepto en sedes diferentes, dependiendo de cuál fuera ésta: la vulneración de la intimidad, el daño del sistema, etcétera.

Y, en cualquier caso, siempre sería difícil entender subsumible en un precepto de estas características el aprovechamiento -sin acceso directo al terminal o a sus contenidos- de los servicios, por ejemplo, de

banda ancha, que el mismo pueda prestar, para lo que sería necesario, lo que también en algún foro se reclama, en un exceso de rigor intervencionista, un tipo que sancionara la simple obtención indebida de prestaciones económicas, sin correlativo perjuicio alguno, que pueda procurar un terminal de comunicación. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 171)”

3.4.1.1.1.4. Delitos de falsificación (falsedades informáticas)

Frente a los delitos de falsedades, refiriéndonos a falsedades informáticas en el ámbito del derecho Penal Español, es importante partir desde el concepto del documento objeto de la falsedad, así determinar si los datos o información digital o virtual tienen esa misma concepción ontológica para determinar la adecuación típica del delito, con los elementos normativos a que haya lugar.

Este caso concreto ha sido estudiado por De La MATA BARRANCO y HERNÁNDEZ DÍAZ en su obra en cita, así:

Los delitos de falsedad, especiales en algún caso, tratan de tutelar la credibilidad social de que gozan ciertos signos, objetos o formas y, quizás de modo más preciso, la propia función del documento en el tráfico jurídico.

El problema fundamental que se plantea en este ámbito en los contextos digitales es únicamente el de si en el concepto de documento a que se refieren los artículos 392 y 395 ó 393 y 396 -en cuanto al uso

de los documentos a que se refieren los dos anteriores- han de comprenderse los datos que se transmiten a través de redes informáticas.

El Convenio de Budapest, en su art. 7, dedicado al delito de falsedad informática, que junto con el art. 8 previsto para la estafa informática, integra el Título que el mismo destina a lo que en él se denominan «infracciones informáticas», en su sentido por tanto más estricto -según el criterio del Convenio, a nuestro juicio erróneo-, atendiendo específicamente este ámbito obliga a sancionar «la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos», aceptando que los Estados puedan reservarse el derecho a exigir un ánimo cualquiera para que nazca la responsabilidad penal.

Si bien es cierto que el art. 26 del Código Penal, que es el que define el concepto de documento, no hace alusión alguna a esta cuestión, sí exige considerar documento sólo al soporte material que exprese o incorpore datos, hechos o narraciones con cualquier tipo de relevancia jurídica.

El material del soporte es indiferente mientras permita incorporar tales datos, hechos o narraciones; pero es necesario el mismo para garantizar la perdurabilidad del documento, que es lo que le otorga credibilidad y funcionalidad en el tráfico jurídico.

Hoy la doctrina y jurisprudencia penal aceptan sin discusión que el soporte informático permite integrar el concepto de documento³³⁸, siempre por supuesto que, como en cualquier otro supuesto, se materialice una declaración de voluntad atribuida o atribuible a persona determinada o determinable destinada al tráfico jurídico o que pueda incorporarse a él³³⁹.

La única cuestión a debatir es si la información -de imagen, texto o sonido- no contenida en un diskette, unidad de USB o soporte físico de otro tipo puede aceptarse como documento, lo que no parece plantear mayor problema siempre que la misma pueda ser visualizada o escuchada sin que se necesite su transcripción impresa.

En el caso de los sistemas de biometría e identidad digital, ningún problema hay en que se puedan falsificar aquellos soportes que incorporen algún tipo de información relevante para el sistema o utilizar los ya falsificados; la tutela penal debiera ser plena en estos casos.

Tampoco parece que en cuanto a las conductas a que alude el Convenio haya laguna alguna en la legislación española, que no requiere ulterior intencionalidad, con independencia de que, por regla general, la falsificación o la utilización vendrán asociadas a la comisión de un delito posterior, patrimonial o contra la intimidad, cuya penalidad habrá de entrar en concurso, normalmente de infracciones, con la que

³³⁸Sobre el concepto de documento electrónico, a estos efectos, en detalle, DE URBANO CASTRILLO, «El documento electrónico: aspectos procesales», pgs. 568 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 172. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³³⁹Por todos, MIR PUIG, «Sobre algunas cuestiones del derecho penal en Internet», pgs. 283 y ss. Véase la crítica de PICOTTI, «Internet y Derecho Penal», pgs. 330 y ss., sin embargo, a la asimilación absoluta del documento tradicional al documento en soporte informático hecha por el legislador italiano, considerando que no se tiene en cuenta con ella las peculiaridades de este último. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 173. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

corresponda por el delito de falsedad cometido. En todo caso, en lo que es la falsificación en sí cabe hablar de un delito contra sistemas informáticos, siempre que de lo que se trate sea de alterar la veracidad o la autenticidad de los datos informáticos; no, por supuesto, si lo que se falsifican son meros soportes informáticos, en cuyo caso -como en general en todos los supuestos de piratería informática- habrá que remitirse, claro está, a los delitos contra la propiedad intelectual o, en su caso, industrial.

Llama la atención, por otra parte, la previsión del art. 400, cuyo contenido se acoge de modo similar, en otros contextos, en el art. 248.3 ó 270.3, en cuanto punición de actos preparatorios, que también prevé el Convenio pero sólo para las «infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos» de sus arts. 2 a 6, entre los que no se incluyen las falsedades informáticas.

Siguiendo las indicaciones de la Decisión Marco 413/2001, de 28 de mayo de 2001, del Consejo de la Unión Europea, se prevé la sanción, con un concepto restrictivo y extensivo de falsificación al mismo tiempo, de la copia o reproducción de las tarjetas, pero no, por ejemplo, de la manipulación de tarjetas auténticas con finalidades fraudulentas -por ejemplo, incorporando datos obtenidos ilícitamente a la banda magnética de la tarjeta auténtica, que, en su caso, habría que reconducir al ámbito de la estafa-; también de la tenencia «en cantidad que permita suponer están destinadas a la distribución o tráfico», anticipando la intervención penal aunque sin llegar al extremo de sancionar la posesión para su posterior uso propiamente mercantil; y, finalmente, del uso en perjuicio de otro y a sabiendas de la falsedad de la tarjeta falsificada, de forma similar a lo que penalizan los arts. 393 y

396. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 171-174)

Vemos entonces a modo de conclusión, que para que la información contenida en medios digitales tenga el concepto de documento debe contener la manifestación de la voluntad del sujeto, es decir, la falsedad recae sobre la modificación o adulteración de la voluntad que un sujeto ha manifestado a través de un medio, que para este caso sería el documento.

3.4.1.1.2. Delitos cometidos a través de la informática contra sistemas informáticos o informaciones digitalizadas

3.4.1.1.2.1. Delitos de encubrimiento y revelación de secretos (accesos informáticos ilícitos, interceptación de comunicaciones, intrusismo informático)

La dogmática penal Española, en este caso en cabeza de De la Matta Barranco y Hernández Díaz, se ha pronunciado frente a la protección penal del derecho a la intimidad, así:

En relación con los delitos que tratan de tutelar la intimidad, en lo que a la securización digital se refiere, los mismos deben poder prevenir la realización de conductas vinculadas al apoderamiento de datos de carácter personal contenidos en archivos informáticos, la interceptación de comunicaciones telemáticas y el acceso y en su caso distribución de

*datos contenidos en ficheros automatizados*³⁴⁰. Conductas también previstas por el Convenio de Budapest, básicamente en su art. 3 y, con matices, en sus arts. 2 y 4, dedicados respectivamente a la «interceptación ilícita», el «acceso ilícito» y los «atentados contra la integridad de los datos», dentro de un Título 1 dedicado a las «infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos». (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Según el autor citado, si el delito de encubrimiento y revelación de secretos posee dentro de sus características la obligación superior de prevenir la realización de conductas atentativas contra el bien jurídico tutelado que protege, entonces nos encontramos frente a un delito de peligro, en el cual la tentativa de su realización puede ser objeto de sanción penal.

*Son estos ilícitos los que, por referirnos a supuestos habituales, permiten penalizar el apoderamiento de mensajes de correo electrónico o de cualesquiera otros documentos de carácter informático*³⁴¹, esto es, contenidos en soportes informáticos o distribuidos a través de medios informáticos, así como, en relación a casos más tradicionales, reactivados con las nuevas tecnologías de la comunicación, la interceptación de comunicaciones telemáticas y la utilización de artificios técnicos de acceso a señales de comunicación telemáticas.

³⁴⁰Véase, sobre esta cuestión, ROMEO CASABONA, «LOS datos de carácter personal como bienes jurídicos penalmente protegidos», pgs. 179 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 175. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁴¹Explica FERNÁNDEZ TERUELO, *El ciberbercrimen. Los delitos cometidos a través de Internet*, pg. 125, que por mensaje de correo electrónico, en sentido amplio, ha de entenderse «cualquier fórmula que posibilite la comunicación entre sujetos a través de la Red»; también ROMEO CASABONA, «La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de Internet», pg. 80. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 175. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

Es lo que en el Código español penaliza el art. 197.1, en sus incisos 1º y 2º, sólo a instancia de parte. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Ahora bien, de entrada hay que señalar que el precepto, que contempla únicamente la vertiente dolosa de estos comportamientos -no imprudente-sanciona tales conductas únicamente cuando se realicen «para descubrir los secretos» o «para vulnerar la intimidad de otro», elemento subjetivo que habrá que probar. Y, si se opta por esta vía, de nuevo habrá que negar -también en esta sede- la posibilidad de sancionar las conductas de mero intrusismo (hackers blancos)³⁴² - salvo, claro está, que las mismas conlleven “el inicio de ejecución de un supuesto de apoderamiento de datos de carácter personal- y sí únicamente las de los accesos no autorizados aprovechando agujeros de seguridad u otras técnicas de hacking -sniffers, troyanos- siempre que se actúe con aquella finalidad. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Es importante resaltar frente al planteamiento del autor en cita que dentro de esta categoría de injustos penales no cabe su penalización cuando no se cumpla con el elemento subjetivo del dolo, lo que quiere decir que dentro de

³⁴²Sobre la defensa de esta opción legal, detenidamente, MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pgs. 74 y ss.; más recientemente, también MATELLANES RODRÍGUEZ, «Vías para la tipificación del acceso ilegal a los sistemas informáticos», pgs. 64 y ss. A favor de la incriminación de estas conductas, en cambio, DE ALFONSO LASO, «El hacking blanco. Una conducta ¿punible o impune?», pgs. 516 y ss.; o GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo Código Penal», pgs. 299 y ss. MAGRO SERVET, «La responsabilidad civil y penal en el campo de la informática», pgs. 398 y ss., considera no sólo que estas conductas deben ser penalizadas, sino que, actualmente en Códigos como el español, cuya lectura -y a nuestro juicio incluso interpretación extensiva- carece de dejarlas fuera, se pueden considerar incriminadas entre los delitos contra la intimidad (p. ej., en el art. 197.2 del citado texto). Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 175. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

las modalidades de ejecución no puede contemplarse la culpa o la preterintención para su tipificación.

En el art. 197.2, también perseguible a instancia de parte, se sanciona el apoderamiento, utilización o modificación de «datos reservados» registrados en ficheros o soportes informáticos, electrónicos o telemáticos o el acceso a ellos sin autorización, conductas que afectan a la confidencialidad y la integridad de tales datos, que puede cuestionarse, no obstante, deban sancionarse sólo cuando exista perjuicio, o intención de causarlo, para el titular o para un tercero³⁴³, como sucede con las conductas del primer apartado y con las del último inciso del segundo, esto es, todas menos las de mero acceso. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Quiere decir lo anterior que para que se logre tipificar esta conducta, debe contarse con el elemento determinador del objetivo del sujeto activo, es decir, cuando el acceso a los datos se haga con la finalidad de causar un perjuicio al titular de la información o a un tercero.

En el art. 197.5 las conductas sancionadas son las mismas, pero referidas a datos que afectan a lo que se considera el núcleo esencial de la intimidad de las personas (ideología, religión, creencias, salud, origen racial o vida sexual) con lo que en aquél, que prevé pena menor, habrán de incluirse cualesquiera otras que no sean de público conocimiento. El art. 197.3 sanciona con pena agravada la difusión de los datos -cualquiera de ellos- y el art. 197.4, único perseguible de

³⁴³Véanse DOVAL PAÍS/JAREÑO LEAL, «Revelación de datos personales, intimidad e informática», pgs. 1486 y ss. Sobre el posible sentido de este perjuicio, Ruiz MARCO, *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*, pgs. 83 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 177 En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

oficio, agrava también la conducta de quien estando encargado o siendo responsable de este tipo de ficheros o soportes informáticos, electrónicos o telemáticos, realiza alguna de las conductas descritas (ténganse en cuenta también los arts. 198, 413 ss., 534 ss. y 598 ss.)³⁴⁴. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

En todo caso, como previsión autónoma o dentro del ámbito de los delitos contra la intimidad, es el único precepto que podría acoger el mero intrusismo informático, el acceso de quien únicamente pretende demostrar pericia, motivaciones políticas no punibles, etc., tratando de garantizar más que otra cosa, y en el ámbito de lo que se conoce como securización digital, un uso libre de injerencias ajenas de los sistemas informáticos. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

3.4.1.1.2.2. Delitos contra el secreto de empresa (espionaje informático industrial)

En este momento investigativo vemos como la legislación española se ha preocupado por la protección penal de los bienes jurídicos tutelados en el ámbito económico, es de esta forma que tutela la capacidad competitiva de las empresas dentro del derecho de última ratio, y teniendo en cuenta que los avances tecnológicos permiten un mayor acceso a la información industrial y

³⁴⁴Sobre el mayor desvalor de estos supuestos, MORALES PRATS, «La protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995», pg. 179. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 177 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

empresarial por parte de cualquier sujeto, incluso ajeno a las compañías, se evidencia la necesidad de su protección, así:

“Con un contenido similar, pero en el ámbito de tutela no de la intimidad³⁴⁵, sino del buen funcionamiento del mercado y de las instituciones que le son consustanciales -entre ellas, la capacidad competitiva de la empresa-, el art. 278, en sus diferentes números, sanciona como delito común perseguible también a instancia únicamente de parte, lo que se conoce como conductas contra el secreto de empresa o de espionaje industrial³⁴⁶, que, como en ocasiones se ha destacado, con la implantación de Internet pueden llevarse a cabo por cualquier persona ajena a la empresa atacada³⁴⁷.(De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Aclara el autor en cita cuando dice *perseguible a instancia únicamente de parte*, que es un delito donde el afectado (empresa) es quien debe iniciar la acción penal a través de la denuncia pues ha sido el afectado con la el injusto cometido.

³⁴⁵MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, pgs. 145 y ss., explica acertadamente la inadecuación de la vinculación de estas conductas con la tutela de la intimidad, cuando tienen que ver más con intereses de carácter patrimonial o económico. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 179 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁴⁶Por todos, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, pgs. 102 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 179 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁴⁷Así, RODRÍGUEZ MOURULLO/LASCURAÍN SÁNCHEZ/ALONSO GALLO, «Derecho penal e Internet», pg. 286, aunque cuando como subrayan GALÁN MUÑOZ, «Expansión e intensificación del derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», pg. 19, o GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo Código Penal», pg. 293, estamos ante ataques cometidos todavía hoy mayoritariamente por *insiders*. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 179 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

Adicionalmente en este tipo penal se encuentra un elemento normativo fundamental para lograr su tipificación y este es que los datos, documentos, o soportes informáticos que sean afectados, divulgados, alterados o interceptados deben contener información de tipo secreto relacionada con la competitividad de la empresa y así mismo utilizada de forma perjudicial por la competencia, así lo define el autor en cita, cuando dice:

Hablamos de conductas de apoderamiento de datos, documentos electrónicos o soportes informáticos donde se incluyan secretos de empresa o de interceptación de comunicaciones que afecten al mismo, realizadas con intención de descubrir tales secretos, que han de recaer sobre aspectos de la vida de la empresa -comercial, de desarrollo e investigación, de innovación, fiscal, industrial, laboral, publicitario, etc.- que tengan valor competitivo, esto es, cuyo conocimiento pueda ser valioso para los competidores, y no sean de público conocimiento³⁴⁸, con la discusión, también aquí, sobre la exigencia o no de alguna finalidad y la consiguiente impunidad, o no, del puro intrusismo. Téngase en cuenta, sin embargo, que no se sanciona la destrucción, alteración u ocultación de la información, como sí ocurre en el caso de la intimidad (art. 197.2). (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 174-179)

Ahora De La Mata y Hernández se han pronunciado frente a la sanción penal del delito de apoderamiento o destrucción de soportes informáticos, remitiéndola a los delitos contra el patrimonio económico que regulen cada caso concreto.

³⁴⁸Entre otros, FERNÁNDEZ TERUELO, *El ciberbercrimen. Los delitos cometidos a través de Internet*, pg. 147. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 180 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

Finalmente, que el art. 278.3 alude también, aquí ya expresamente, a la sanción del apoderamiento o destrucción de los soportes informáticos que incorporan el secreto de empresa, pero remitiéndola a la aplicación del delito patrimonial correspondiente, en el intento por abarcar el desvalor total de la conducta que puede llevarse a cabo. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:180)

3.4.1.1.3. Delitos cometidos a través de sistemas informáticos

3.4.1.1.3.1. Delitos de defraudación (estafas o fraudes informáticos)

La legislación española consagra el delito de estafa como un engaño de gran envergadura que logra llevar al sujeto pasivo al error que como consecuencia genera un detrimento patrimonial a este mismo o a un tercero.

Así lo definen De la Mata Barranco y Hernández Díaz en su obra en cita:

La estafa se define por la utilización de un engaño bastante que, generador de un error en otro, favorece una disposición patrimonial de éste, en perjuicio propio o de tercero. En este contexto, ha sido largamente debatido el tratamiento que ha de darse a aquellos supuestos en que lo que se produce es una actuación fraudulenta en un aparato, con la que se consigue la disposición patrimonial. Y en el ámbito estrictamente informático, el tratamiento que ha de darse a aquellos supuestos en que se produce una manipulación en sistemas

*digitales con la que se logra una transferencia patrimonial*³⁴⁹. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 180)

Ahora frente al mismo ilícito de la Estafa, visto desde la modalidad de Estafa informática, tenemos que la doctrina penal española en cabeza de los autores en cita vemos que el artículo 248.2 del Código Penal Español tipifica este injusto, así:

“En el caso del derecho español, como en otros, este ámbito de la estafa informática (o, genéricamente, de los fraudes informáticos³⁵⁰) ha sido abordado directamente por el legislador mediante la previsión de un art. 248.2 que expresamente contempla este tipo de supuestos exigiendo únicamente una manipulación informática o artificio semejante con los que se consiga una transferencia patrimonial no consentida en perjuicio de tercero. Aquí tendrán cabida, por ejemplo, tanto la quiebra de los sistemas de seguridad -por ejemplo, de identidad digital-, siempre que con ella se persiga la transferencia de activos descrita, como la obtención de transferencias mediante suplantaciones de identidad.

En cierta medida, los elementos de la estafa informática siguen siendo paralelos a los de la estafa genérica: así, la manipulación informática o artificio semejante equivaldría a la producción de engaño bastante y

³⁴⁹Véanse, entre otros, DE LA MATA BARRANCO, «Utilización abusiva de cajeros automáticos», pgs. 151 y ss.; MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pgs. 38 y ss.; o ROMEO CASABONA, *Poder informático y seguridad jurídica*, pgs. 47 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 180 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁵⁰Sobre el concepto específico de fraude informático, GUTIÉRREZ FRANCÉS, *Fraude informático y estafa*, pgs. 87 y ss.; también, ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pgs. 241 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 181 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

generación del consiguiente error, mientras que la transferencia lograda equivaldría al acto de disposición, siendo común a ambos supuestos la causación de un perjuicio patrimonial. Sin embargo, son diferentes las peculiaridades criminológicas de estos delitos de estafa vinculados a la informática, desde la expansión de Internet, de entre las que se destacan su facilidad de comisión por la posibilidad de anonimato que otorga la red, el gran número de cifra negra que se experimenta, por la ausencia en muchos casos de denuncia -en aras en muchos casos a impedir la pérdida de credibilidad empresarial y social- y el poco coste -y riesgo- que supone para sus autores la puesta en marcha de estos delitos desde la Red³⁵¹. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 180)

Vemos entonces que para el caso español el delito de Estafa informática mantiene los elementos de la Estafa genérica perteneciendo a la categoría de fraudes informáticos, teniendo como elementos normativos adicionales para lograr la tipificación, en palabras de los autores en cita, los siguientes:

“En estas conductas de fraude informático mediante las que se logran transferencias de fondos no consentidas a través de órdenes falseadas o de la alteración del funcionamiento de los programas gestores de las operaciones contables, consideradas por algún autor como el auténtico núcleo del Derecho penal informático³⁵², la manipulación puede producirse en el mismo programa, en cualquier momento del procesamiento o tratamiento automatizado de datos, ya sea en la

³⁵¹Extensamente YAR, *Cybercrime and society*, pgs. 90 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 181 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁵²Véase ROMEO CASABONA, *Poder informático y seguridad jurídica*, pg. 47. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 181 En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

entrada (input) o salida (output), ya en la transmisión a distancia, mediante modem, red, etc., ya en la retroalimentación (feedback) o incluso en la obtención informática, pero personal, de los datos que permiten la transferencia patrimonial.

Por supuesto, no se sanciona únicamente la utilización del sistema para, desde dentro, generar tales disposiciones a través de órdenes no autorizadas que emiten personas autorizadas a dicha utilización o de actuaciones no autorizadas por quienes no tienen permiso para acceder al mismo, sino también la actuación «desde fuera» que, por ejemplo, consigue generar aleatoriamente números de tarjetas de crédito aceptadas para la realización de compras ficticias o que consigue irrumpir en sistemas ajenos para alterar las órdenes de compra, inversión o transferencia de fondos que los sistemas permiten o que, de cualquier otro modo, consiguen quebrar los sistemas de identidad digital generados al efecto de evitar utilizaciones o usurpaciones de identidad no deseadas³⁵³. Siempre, ha de insistirse en ello, desde la perspectiva de la pretensión de causación de un perjuicio patrimonial derivado del correlativo enriquecimiento del infractor.

Las dudas sobre la posibilidad de ubicar este tipo de conductas en el ámbito clásico de la estafa activa la creación del delito de estafa informática³⁵⁴. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 181)

³⁵³Véanse las diferentes conductas fraudulentas que pueden cometerse a través de Internet, con detalle, en FERNÁNDEZ TERUELO, *Ciberdelitos. Los delitos cometidos a través de Internet*, pgs. 27 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 182 En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁵⁴Por todos, ROMEO CASABONA, *Poder informático y seguridad jurídica*, pgs. 47 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 182 En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas

Es así como nace como tipo penal la estafa informática, de la necesidad de adecuar las legislaciones a la realidad del mundo tecnológico, sin embargo no todas las conductas informáticas que involucren engaño a terceros se constituyen este injusto, nacen grandes dudas frente a las conductas que un con engaños informáticos logran obtener servicios gratuitos, adecuándolas típica, antijurídica y culpablemente en otros tipos penales.

Así lo definieron los citados autores:

“Pero, a pesar de ello, y si bien es cierto que lo único que requiere la estafa es la mera transferencia contable, que puede concretarse de las formas más variadas -no sólo obtención de un ingreso ficticio, sino generación de un derecho de crédito o de una orden de pago o cancelación de una deuda, etc.-, es dudoso que este delito permita abarcar conductas en las que no se produce estrictamente una transferencia no consentida de un activo patrimonial; así, por ejemplo, en el supuesto de disfrute gratuito de servicios sin imputación de coste a un tercero, que ha parecido más adecuado remitir a delitos de prestación ilícita de servicios restringidos –en el caso español, el art. 286-, si se dan los elementos que definen su tipicidad³⁵⁵.

Por otra parte, es difícil también entender abarcados por el delito de estafa informática aquellos supuestos en que no se produce manipulación informática o artificio semejante alguno, sino simplemente utilización de claves de acceso obtenidas lícita o ilícitamente, que nos conducen entonces necesariamente a la comprobación de los elementos del tipo básico de estafa (como en el supuesto de obtención de bienes de modo fraudulento de un aparato

³⁵⁵Véase también, por ejemplo, el art. 301a del Código penal danés. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 183. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

automático) o del de robo con fuerza en las cosas, según las diferentes interpretaciones que se han mantenido en relación a este supuesto, o incluso, en su caso, como antes apuntábamos, al delito de prestación ilícita de servicios restringidos del art. 286.

Dentro de esta perspectiva digital del modo de comisión de una estafa, el Proyecto de 2009 introduce también aquí un nuevo precepto, el 248.2.c) -el actual art. 248.2 pasa a ser el 248.2 a) y el art. 248.3 el 248.2.b)-destinado específicamente a sancionar la utilización de tarjetas de crédito o débito, o los datos obrantes en ellas en perjuicio de su titular o de un tercero, tratando de solucionar los supuestos todavía controvertidos de accesos a cajeros mediante utilización no consentida de la tarjeta de un tercero, utilización abusiva de la tarjeta por su propio titular o utilización de tarjeta falseada o alterada o de los datos obrantes en ella, que la doctrina sigue discutiendo si ubicar en el art. 248.1 o en el art. 248.2 o incluso en el 238.57239 pfo. 2³⁵⁶.

Por supuesto, la estafa tradicional -art. 248.1- será de aplicación en todos aquellos casos en que el contexto digital para lo que sirve es únicamente para facilitar, sobre todo en supuestos de fraude en el comercio electrónico, el engaño generador del error, como por ejemplo, en los de estafa de inversiones, que también pueden darse con mayor facilidad en los contextos digitales³⁵⁷, y que el Proyecto de 2009 también aborda específicamente en el art. 282 bis.

³⁵⁶Sobre esta discusión, entre otros, CHOCLÁN MONTALVO, «Fraude informático y estafa por computación»; DE LA MATA BARRANCO, «Utilización abusiva de cajeros automáticos», pgs. 151 y ss.; GALÁN MUÑOZ, *El fraude y la estafa en los sistemas informáticos*, pgs. 744 y ss.; GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo Código Penal», pgs. 260 y ss.; o MATA Y MARTÍN, *Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago*, pgs. 109 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 184. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁵⁷Por todos, RODRÍGUEZ MOURULLO/LASCURAIN SÁNCHEZ/ALONSO GALLO, «Derecho Penal e Internet», pg. 291. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010)

Y, aunque fuera ya tanto de la estafa tradicional como de la informática, pero contemplada ya en muchas legislaciones, el art. 255 contempla como modalidad clásica de fraude patrimonial la defraudación en los sistemas de telecomunicaciones mediante manipulaciones clandestinas: conexiones a redes de pago, alteraciones en la red para disfrutar de servicios no pagados, desconexiones de servidores habituales redireccionados a otros servidores de pago o a otros números telefónicos más costosos, etc., con o sin quiebra de firewalls, con o sin quiebra de sistemas de autenticación digital, con o sin quiebra de cualquier mecanismo de protección frente a usos indebidos.

Finalmente, al art. 256, uso sin consentimiento de cualquier equipo terminal de comunicación, ya se ha hecho referencia en el epígrafe dedicado a los delitos contra los sistemas informáticos, por cuanto lo que refiere no es la causación de un perjuicio patrimonial derivado de la utilización del terminal de comunicación, sino la propia autorización no consentida, causante en sí ella misma de dicho perjuicio. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 180-185)

3.4.1.1.3.2. Delitos relativos al mercado y los consumidores (facilitación o prestación ilícita de servicios restringidos)

El delito de facilitación o prestación ilícita de servicios restringidos dentro de la legislación Penal Informática en España se encuentra enmarcado dentro del grupo de delitos relativos al mercado y los consumidores.

P. 184. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

De la Mata Barranco y Hernandez Díaz se han pronunciado frente a estos injustos penales, manifestando la razón por la que han sido separados de los delitos de estafa, así:

Este tipo de conductas, aludidas en el apartado anterior, tienden a independizarse como se decía de los supuestos clásicos de estafa para pasar a forma parte de tipicidades autónomas, descritas de modo diversos en las diferentes legislaciones, que tratan de abarcar los comportamientos que facilitan el acceso a servicios de radiodifusión sonora o televisiva o a servicios interactivos prestados a distancia, por los que hay que pagar un precio al prestador de los mismos. El nuevo delito del art. 286, incorporado al Código en 2003 y paradójicamente perseguible sólo a instancia de parte -aunque no se precise la denuncia, como dice el art. 287.2, si el delito afecta a intereses generales, que son los que en principio debieran considerarse objeto de tutela de un delito situado entre los relativos «al mercado y los consumidores»- pretende en realidad, al margen de su ubicación sistemática la protección de los intereses de quienes prestan los servicios de comunicación e información referidos. De ahí justamente la remisión penológica al art. 255 en el art. 286.4, y aun cuando en ningún momento se exija perjuicio alguno o, mucho menos, enriquecimiento o incluso ánimo de lucro -dependiendo esto último del número del artículo a aplicar-.

Se sancionan tanto conductas de prestación o facilitación del servicio como de preparación a ello, con fines comerciales -art. 286.1- o ánimo de lucro -art. 286.2- o sin él -art. 286.3-, en un intento por abarcar todo tipo de conductas vinculadas a lo que se conoce como phreaking -incluyendo la del usuario del servicio, siempre no obstante que se sirva de servicios o programas informáticos, por ejemplo, mediante tarjetas clonadas, pero no, en cambio, salvo en una interpretación extensiva del

precepto que no entiendo sin embargo desacertada en este caso, cuando utilice combinaciones de series numéricas ilícitamente facilitadas- con o sin artificios técnicos, y con una redacción que permite abarcar muchos comportamientos hasta ahora sólo de modo forzado vehiculados a través de la estafa del art. 248.1 o de la defraudación del art. 255³⁵⁸. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:186)

3.4.1.1.3.3. Falsedades personales (adopción fraudulenta de identidad digital falsa)

Después de haber analizado las conductas de falsedad en documentos, vemos que la legislación Española se ha encargado de regular la usurpación de identidad dentro de la modalidad de falsedades personales, exactamente bajo el tipo penal de adopción fraudulenta de identidad digital falsa. Para los autores citados anteriormente, la atribución de un estado civil ajeno se convierte en un injusto penal bajo los siguientes preceptos:

“Interesa también en este ámbito al menos aludir a la previsión del art. 401, un tanto incorrectamente ubicado entre los delitos de falsedades, atendiendo la diversidad de objetos de tutela, donde se sanciona la atribución de un estado civil que no es el propio.

Apenas se ha planteado hasta ahora la subsunción de conductas relacionadas con la criminalidad informática en el ámbito de la usurpación de un estado civil ajeno, pero téngase en cuenta que, al

³⁵⁸Vean las consideraciones de LÓPEZ MORENO/FERNÁNDEZ GARCÍA, «La worldwide web como vehículo de delincuencia: supuestos frecuentes», pgs. 449 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 186. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

margen de lo que es el acceso ilícito a soportes informáticos o terminales de comunicación y de la propia falsificación de los equipos que tratan de garantizar su utilización segura mediante el control de la identidad digital de quien accede a ellos, en todas sus variantes, el «hacerse pasar por otro» a través de un contexto digital, a los efectos de la más diversa índole, y siempre que ello tenga algún tipo de desvalor por la relevancia de la actuación, puede subsumirse perfectamente en este tipo. De nuevo aquí con independencia de que a la pena por esta tipología delictiva quepa añadir la que corresponda por la infracción de otra índole que pueda seguir a la adopción de la identidad falsa o incluso la que corresponda por la manipulación que haga posible la suplantación de identidad.

Téngase en cuenta también que el Proyecto de 2009 prevé un nuevo art. 392.2 en que sanciona expresamente el uso de documento de identidad falso, sin especificar el tipo de documento a que se refiere - por tanto, también de contenido digital- y un nuevo art. 400 bis que sanciona asimismo el uso de documento auténtico por quien no esté legitimado para ello. La posibilidad de incluir en esta sede, y al margen de otras ubicaciones en función de la motivación del autor, utilizaciones fraudulentas de documentos con claves de autenticación, passwords, bandas magnéticas con incorporación de datos personales, etc., debería tomarse en consideración. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:187)

3.4.1.1.3.4. Delitos de difusión de contenidos lesivos para intereses diversos: libertad, libertad sexual, honor, correcto funcionamiento del mercado, derechos fundamentales y libertades públicas (delitos de difusión informática: webs de contenido sexual respecto a menores, ciberterrorismo, etc.)

Existe una categoría de delitos dentro de la ley penal española que se encarga de la persecución penal de conductas que atentan contra el mercado, derechos fundamentales y libertades públicas, estas conductas se tipifican como delitos de difusión informática.

En el ámbito de los delitos relacionados con la libertad sexual y más importante aun cuando estas conductas pueden resultar vulneradoras de derechos a menores de edad, los doctrinantes De la Mata Barranco y Hernandez Díaz se han pronunciado en el siguiente sentido:

En el ámbito de la libertad o indemnidad sexual, el Código penal permite contemplar hechos punibles relativos a materiales pornográficos que puedan tener una especial vinculación con medios informáticos: en el art. 186 en relación a supuestos de pornografía dirigida a menores - también en el art. 185 en cuanto a ejecución de actos de exhibición obscena ante menores- y en el art. 189 en relación a supuestos de pornografía infantil. En ninguno de ambos preceptos se menciona expresamente el ámbito informático, pero al sancionarse la venta, difusión o exhibición, en un caso, y la elaboración, producción, venta, distribución, exhibición, facilitación de las anteriores conductas, financiación, posesión con aquellas finalidades o para uso propio, sin

diferenciar el tipo de soporte e incluso utilizando la expresión en el caso del art. 189.1 a) «cualquiera que sea su soporte», la regulación perfectamente permite sancionar la realización de cualesquiera de los anteriores comportamientos a través de redes informáticas.

El problema que plantea la utilización de estos preceptos, prescindiendo de discusiones habituales en su seno ajenas a lo estrictamente informático, es, en primer lugar, y en el caso del art. 186, que se requiere utilización de un medio directo lo que, aunque no impediría la sanción de conductas de venta, difusión o exhibición de material entre menores a través de correos, foros o chats con menores concretos, imposibilita la prevención cuando se utilizan páginas no dirigidas expresamente a menores. A ello puede añadirse la cuestión del posible desconocimiento de la edad del usuario.

En cuanto a la aplicación del art. 189.1, que permite sancionar conductas de elaboración de material pornográfico con menores³⁵⁹ a través de procedimientos informáticos y de posterior distribución en sentido amplio de dicho material, el problema va a plantearse - solucionada la cuestión de la jurisdicción, al tratarse de delitos de justicia universal, perseguibles sea cual sea el lugar donde se cometan³⁶⁰- a la hora de determinar, sobre todo, la autoría y el concepto de «facilitación», que, interpretado en sentido amplio, permite la sanción de cualquier tipo de comportamiento (creación de listados,

³⁵⁹Sobre la propia complejidad del concepto, especialmente en los contextos digitales, FERNÁNDEZ TERUELO, *Ciberdelitos. Los delitos cometidos a través de Internet*, pgs. 68 y ss.; o MORALES PRATS, «Pornografía infantil e Internet: la respuesta penal: la respuesta en el Código penal español», pgs. 178 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 189. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶⁰A pesar de ello, véanse, no obstante, los problemas de persecución de estas conductas que destaca MORALES PRATS, «El derecho penal ante la pornografía infantil en Internet», pgs. 114 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 189. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas

información a terceros, etc., e incluso en opinión de algunos -hoy por hoy, minoritaria- la procuración de medios técnicos). (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:191)

Ahora, frente a los delitos de apología al delito, terrorismo, delitos contra el honor, publicidad engañosa, entre otros encontramos de gran importancia el pronunciamiento de los autores en cita, vemos que dan algunos visos sobre los ciberdelitos como se han planteado en la presente investigación, sin embargo no se adentran en establecer un mecanismo o solución al problema de la jurisdicción y competencia para su juzgamiento, como se muestra:

Si algo caracteriza en esta nueva época la problemática penal de Internet es la amplia posibilidad que ésta presta para la difusión de contenidos lesivos de intereses objeto de tutela penal³⁶¹, en el ámbito de los delitos contra el honor³⁶², la publicidad engañosa³⁶³, la apología de la violencia³⁶⁴ o el terrorismo³⁶⁵. Por supuesto, y al margen de cuestiones de competencia de jurisdicción, etc., si bien pudiera parecer que este ámbito de criminalidad no afecta ni a lo que es el ámbito de la securización digital en sí ni al del correcto uso de los sistemas

³⁶¹Véase LÓPEZ ORTEGA, «Libertad de expresión y responsabilidad por los contenidos en Internet», pgs. 106 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 187. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶²Por todos, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, pg. 146. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 187. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶³Detenidamente, SIERRA LÓPEZ, *Análisis jurídico-penal de la publicidad engañosa en Internet*, pgs. 227 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 187. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶⁴Específicamente, YAR, M. *Cybercrime and society*, pgs. 97 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 187. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶⁵Véase, entre otros, MORALES PRATS, «LOS ilícitos en la red (II): pornografía infantil y ciberterrorismo», pgs. 273 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 187. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

informáticos conforme a los fines que les son propios -no estamos en el ámbito de infracciones contra contextos digitales-, los problemas pueden surgir cuando sistemas de titularidad o uso compartido se utilizan para dicha difusión -o recepción-, en el contexto de la dificultad que puede generar la determinación de las responsabilidades derivadas de ello³⁶⁶.

En todo caso es ésta ciertamente una problemática menor en comparación con lo que implican estos medios para la proliferación de actuaciones delictivas o para su mayor facilidad de comisión o de ocultamiento³⁶⁷. La ventaja que ofrecen las tecnologías de la comunicación para la realización de determinada clase de conductas, no sólo de opinión, que será lo más frecuente -delitos de amenazas, contra el honor, de provocación a la discriminación, el odio o la violencia o de terrorismo-, sino de afección a ámbitos especialmente sensibles como el de la tutela de la libertad sexual en cuanto a la protección de los menores se refiere, es indudable. A éste último ámbito cabe hacer una especial referencia por ser quizás aquél en que mayor incidencia ha tenido de hecho el desarrollo de este tipo de tecnología³⁶⁸. (De LA MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:191)

³⁶⁶A este respecto, en detalle, la completa monografía de GÓMEZ TOMILLO, *Responsabilidad penal v civil por delitos a través de Internet. Especial consideración del caso de los proveedores de contenidos, servicios, acceso y enlaces*. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 188. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶⁷Por todos, MORALES PRATS, «Pornografía infantil e Internet: La respuesta en el Código Penal español», pgs. 200 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 188. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁶⁸Sobre el aumento de la pornografía infantil motivado por la implantación de Internet, por todos, de nuevo MORALES PRATS, ob. cit., pgs. 180 y ss.; también, del mismo autor, «La intervención penal en la red. La represión penal del tráfico de pornografía infantil: estudio particular», pgs. 119 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 188. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

3.4.1.1.4. Delitos contra la gestión de derechos digitales

En este aparte investigativo se identifican los delitos contra la gestión de derechos digitales dentro de la legislación penal española, teniendo en esta categoría aquellas conductas que atentan contra la propiedad intelectual e industrial, donde se hace referencia clara a las creaciones o invenciones que constituyen medios informáticos, software o medios digitales o aquellas que reposan en estos. Así lo definieron De la Mata Barranco y Hernández Díaz:

La tutela de la propiedad intelectual e industrial, como interés merecedor y necesitado de protección penal, se debe garantizar frente a los ataques más graves para el conjunto de facultades que se derivan de la creación de obras de diversa naturaleza, entre las que están, por supuesto, las que hacen referencia a programas de ordenador, patentes, modelos de utilidad, topografías de semiconductores u otras contenidas en soportes digitales o transmitidas a través de ellos³⁶⁹.

Sin que exista una expresa alusión a la perspectiva informática en la descripción de los distintos delitos y faltas que en el Capítulo XII del Libro XIII se ocupan en el Código Penal, dentro de los delitos contra el patrimonio, de la tutela de la propiedad intelectual e industrial, salvo en la referencia del art. 270.3, es en la descripción genérica de los distintos comportamientos de los arts. 270 y siguientes donde han de tratar de ubicarse las conductas que puedan materializar los riesgos idóneos para menoscabar los derechos que se derivan de la gestión de derechos digitales. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:192)

³⁶⁹Ampliamente, MIRÓ LLINARES, *Internet y delitos contra la propiedad intelectual*, pgs. 28 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 192. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

Aun cuando doctrinalmente existe una diferenciación clara de estos delitos frente a aquellos que atentan contra el patrimonio económico, procesalmente tenemos que estas conductas deben adecuarse jurídicamente a los tipos penales vigentes en la legislación de España, con el propósito de que su persecución penal y la materialización de la política criminal del Estado sea efectiva.

3.4.1.1.4.1. Delitos contra la propiedad intelectual (pirateo informático)

Los delitos contra la propiedad intelectual, en palabras de los autores previamente citados y desde el ámbito procesal son *perseguidos de oficio en la actualidad, refieren en este ámbito, entre otras, las conductas denominadas de pirateo informático*³⁷⁰ *frente a obras originales y exteriorizadas de alguna manera para que hayan podido ser conocidas por terceros*³⁷¹. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 192)

Tenemos entonces que en el código Penal Español, *el art. 270.1 permite sancionar copias no autorizadas de obras de cualquier tipo o distribución de ellas, «fijadas en cualquier tipo de soporte o comunicadas a través de cualquier medio»*; tenemos en este tipo penal un elemento adicional que permite su persecución y recae en que *aun sin mención expresa del*

³⁷⁰Detenidamente, distinguiendo entre los intereses protegidos por el sistema de propiedad intelectual y el sistema americano de *copyright*, de nuevo MIRÓ LLINARES, *La protección penal de la propiedad intelectual*, pgs. 485 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 192. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁷¹Véase MATA Y MARTÍN, *Delincuencia informática y derecho penal*, pg. 83; igualmente, MIRÓ LLINARES, *La protección penal de la propiedad intelectual*, pgs. 271 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 192. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

legislador, ningún problema hay para incluir en el precepto actuaciones delictivas vinculadas a programas de ordenador o informaciones de cualquier naturaleza distribuidas a través de red -comunicaciones de texto, audio o vídeo- respecto de las que existan derechos de autor. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:192)

Frente a la protección especial a los derechos de autor, la doctrina española se ha pronunciado, en los siguientes términos:

En lo que concierne específicamente a la protección de los derechos de autor sobre programas de ordenador, definidos en el art. 96.1 LPI, la misma se efectúa a través de su equiparación -a estos efectos- a las obras literarias³⁷², comprendiendo tanto la que puede existir sobre el software en sí como la que exista sobre su documentación técnica y manuales de uso, ya en relación a los derechos de creación de la obra (plagio, distribución o comunicación -es menos relevante aquí la en otros ámbitos fundamental conducta de reproducción-), ya a los de su explotación (distribución y transformación no consentida de la obra, al margen de la reproducción y la comunicación pública)³⁷³.

Siempre, en todo caso, que las conductas tengan relevancia para afectar a los derechos de propiedad intelectual y no se agote su

³⁷²No obstante, sobre la imposibilidad de identificación entre unos y otras, GÓMEZ MARTÍN, «La protección penal de los derechos de autor sobre los programas informáticos: un ejemplo de la naturaleza patrimonialista de los delitos contra la propiedad intelectual en el CP de 1995», pgs. 158 y ss. . Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 193. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

³⁷³Detenidamente, MATA Y MARTÍN, «Criminalidad informática: una introducción al cibercrimen», pg. 11. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 193. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

*desvalor en la utilización privada de lo que se copia o distribuye*³⁷⁴. Suponiendo que en cuanto al objeto material de la conducta podamos estar en el ámbito de lo que trata de tutelar la Ley de Propiedad Intelectual y que en lo que concierne a las modalidades de la conducta podamos entender que se ha producido, por ejemplo, un plagio, una reproducción o una distribución -con todos los supuestos conflictivos que en este tema se presentan en los contextos digitales- el precepto exige explícitamente además el actuar con ánimo de lucro y en perjuicio de tercero, sin que puedan entenderse comprendidos en el delito los supuestos en que el lucro procede exclusivamente de la ausencia de desembolso por parte de quien utiliza en beneficio propio un producto - con el correlativo lucro cesante para el titular del derecho-, en la absoluta privacidad. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010:192)

3.4.1.1.4.2. Delitos contra la propiedad industrial

En la doctrina penal española existe una diferenciación entre los delitos de propiedad intelectual y propiedad industrial, teniendo como base el objeto material o bien jurídico tutelado.

De carácter absolutamente similar a los delitos contra la propiedad intelectual la única diferencia con ellos de los delitos relativos a la propiedad industrial viene dada por el distinto objeto del delito, sujeto

³⁷⁴En este sentido, por todos, MATA Y MARTÍN, «Perspectivas sobre la protección penal del software», pgs. 143 y 148 y ss., desde el respeto a los principios de subsidiariedad y de fragmentariedad del Derecho penal. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 193. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas

en un caso a derechos de autor, sujeto en otro a la normativa sobre propiedad industrial en la que tendría cabida, por ejemplo, la tutela del nombre de dominio en Internet o cualquier mecanismo de securización diseñado para su explotación comercial.

En este sentido, y obsérvese que la descripción típica es muy parecida en el caso de los arts. 270.1 y 273.1, 2 y 3 y en el caso de los arts. 270.2 y 274.1, e idéntica en el caso de los arts. 271 y 276, la propiedad industrial lo que básicamente refiere son invenciones -ya sea en cuanto a un objeto patentado ya en cuanto al procedimiento para crearlo, también patentado-relacionadas con el ámbito económico, comercial o industrial de determinados productos y lo que en Derecho penal se ha de tutelar es, como ya se ha señalado, «la exclusividad en el uso de tales invenciones o signos distintivos como presupuesto para defender la capacidad competitiva de la empresa y así también los intereses de los consumidores»³⁷⁵.

Acostumbra a explicarse que en lo que afecta a la propiedad intelectual el autor concibe y aplica lo concebido, siendo además la creación de una obra un fin en sí misma, sin perjuicio de su valor de mercado, mientras que cuando de propiedad industrial se trata la originalidad y personalidad de la creación se somete a la finalidad de proporcionar un servicio o utilidad, que a su vez cumplirá el objeto concebido, que podrá ser producido a gran escala por otros, lo que no es imaginable en la creación intelectual o artística. En todo caso, se admite que existen objetos problemáticos, difíciles de encajar en uno u otro tipo de propiedad, como justamente los programas de ordenador, por ejemplo, que por decisión legal corresponden al ámbito de la propiedad

³⁷⁵MATA Y MARTÍN, «Criminalidad informática: una introducción al cibercrimen», pg. 12. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 196. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

intelectual, como recoge el art. 10 de la Ley de Propiedad Intelectual, a pesar de que perfectamente podrían considerarse objetos de propiedad industrial. Obsérvese, en todo caso, que las penas previstas en los arts. 270 y siguientes, por una parte, y 273 y siguientes, por otra, son las mismas.

Interesa, por último, simplemente llamar también la atención sobre la expresa alusión en el art. 273.3 a la tutela de la topografía de productos semiconductores por su vinculación directa, aunque no sólo, al ámbito de la digitalización. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 196-197)

3.4.1.2. Un ejemplo de delitos informáticos: delitos contra sistemas y datos en el Código Penal Español ¿delitos de daños?

En este caso se hace indispensable realizar una clara distinción entre el software y el hardware dentro de los equipos informáticos teniendo como software los componentes lógicos y datos, mientras que el hardware compone los elementos externos del equipo informático, en palabras de De la Mata Barranco vemos:

En cuanto al ataque a los componentes lógicos del sistema -al software-, éste puede realizarse de un modo básico, tradicional, físico, ajeno a lo que es la utilización de las TICs: por ejemplo, golpeando el ordenador, mojándolo, quemándolo, introduciendo cuchillas en la CPU³⁷⁶; pero también puede realizarse a través de medios comisivos

³⁷⁶Alude ya a esta posibilidad CORCOYBIDASOLO, «Protección penal del sabotaje informático. Especial consideración de los delitos de daños», pg. 1002. Citado en: De la MATA

novedosos, vinculados al desarrollo de las TICs: así, introduciendo virus, troyanos, gusanos, etc. En ambos casos podrá afectarse el funcionamiento del sistema y/o la disponibilidad de los datos contenidos en él.

En el caso de estas últimas modalidades comisivas, las mismas se han diversificado tanto que es necesario para entender de qué estamos hablando precisar algunos de los conceptos de la nueva terminología informática referida al modo en que puede producirse el posible ataque -y daño- informático.

Así, se habla de software malicioso o malware para describir un conjunto de códigos y programas, que, introducidos en un sistema informático, originan problemas de utilización u operatividad del mismo -de sus programas de funcionamiento- o alteración o borrado de datos.

Los crashprograms programas destructores hacen referencia a las rutinas (virus, gusanos, conejos, troyanos, etc.) encargadas de destruir gran cantidad de datos en un corto espacio de tiempo³⁷⁷. Los virus son códigos maliciosos creados para alterar un sistema informático que necesitan un programa anfitrión para reproducirse y transmitirse, al que se adhieren para su ejecución. Los gusanos (worms) son piezas independientes de software que a diferencia de los virus son capaces de reproducirse a sí mismos y de autotransmitirse. Los conejos o bacterias son programas que, si bien en principio no dañan el sistema,

BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 202. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁷⁷Ampliamente, SIEBER, «Documentación para una aproximación al delito informático», pg. 75. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 203. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

se autoreproducen ocupando toda la memoria del sistema que, de esta forma, bloquean. Los troyanos son un software malicioso que, oculto en un programa benigno o útil, se introduce en el sistema informático (incluso en teléfonos móviles o PDAs); una vez dentro del sistema, pueden generar un gran número de disturbios o daños en el mismo (borrado o daño en los datos o programas, utilizar el sistema para realizar ataques de denegación de servicios, robar datos y contraseñas, abrir puertas traseras para permitir a los atacantes controlar el sistema y convertir el ordenador en un zombi al servicio de éstos, etc.), lo que les convierte en especialmente peligrosos; los troyanos, en principio, no son capaces de reproducirse a sí mismos, pero, aun así, son en la actualidad la amenaza más importante, cuantitativamente hablando, en los ataques realizados a través de Internet, en detrimento de los virus tradicionales, que van perdiendo importancia³⁷⁸.

Un nuevo tipo de troyano es el denominado Backdoor(puerta trasera) que permite a un atacante tomar el control remoto del sistema infectado para llevar a cabo una gran diversidad de acciones: espiar el escritorio remoto, realizar capturas de pantalla o de la webcam, subir o descargar archivos, alterar el funcionamiento normal del sistema, etcétera.

Es destacable también otro novedoso tipo de ataque que ha surgido en los últimos años, el de los denominados blendedthreats, especialmente

³⁷⁸Según datos extraídos del Estudio sobre Seguridad de la Información y e-Confianza de los hogares españoles realizado por el Instituto Nacional de Tecnologías de la Comunicación (INTECO), publicado en junio de 2007 en su página www.inteco.es, las mayores amenazas a los sistemas informáticos, por su incidencia y gravedad, proceden en la actualidad de los troyanos (amenaza para el 50,3% de los equipos). La tradicional amenaza de los virus, en cambio, afecta al 10,1% de los ordenadores y sólo representa un 1,2% de las variantes de *malware* encontradas; esta pérdida de importancia se debe, por un lado, a la eficacia de los sistemas antivirus y de sus actualizaciones automáticas y, por otro, al abandono del desarrollo de virus a favor, sobre todo, de dichos troyanos. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 203. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

peligrosos por combinar las características de virus, gusanos y troyanos con las vulnerabilidades de Internet y de sus servidores para crear, transmitir y propagar los ataques³⁷⁹. El ataque se materializaría, por ejemplo, además de con el lanzamiento de un ataque DoS, con la instalación de un backdoory con el daño de un sistema local. Las amenazas mixtas, además, pueden utilizar múltiples modos de transporte: así, el e-mail, IRC o archivos compartidos en redes p2p. Y el ataque no se limita a un solo acto, pudiendo modificar un ataque mixto, por ejemplo, archivos.exe, archivos, html el registro al mismo tiempo.

Las bombas lógicas son rutinas introducidas en un programa para que, al realizar una determinada acción -por ejemplo la copia del mismo-, se produzcan alteraciones o daños en el programa. Las bombas de tiempo, como las lógicas, son rutinas introducidas en programas o archivos, pero para que se produzca una alteración del programa o daño al mismo en un momento determinado, al llegar una fecha concreta o pasar un plazo de tiempo establecido al efecto.

Los ataques de denegación de servicios (DoSAttacko denial of service) son conductas tendentes al bloqueo de un sistema informático mediante la saturación del mismo. Este bloqueo conlleva que los usuarios del sistema informático no puedan acceder a él o a ciertos recursos o datos del mismo durante el período de saturación, que a menudo se produce mediante un sistema de acumulación de peticiones de información que se rechazan automáticamente.

Son muchos otros los ataques que pueden producirse contra un ordenador -por ejemplo, últimamente prolifera el adware (software que

³⁷⁹Véanse HUGHES/DE LONE, «Virus, Worms, and Trojan Horses. Serious Crimes, Nuisance or both?», pg. 81. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 203. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

muestra publicidad en ventanas emergentes, banners, etc., no solicitada), recopilando en ocasiones información sobre los hábitos de navegación de los usuarios para luego redirigirles a la publicidad coincidente con sus intereses-, pero que no tienen por qué afectar al correcto funcionamiento del sistema.

Como sinónimo de daño informático se utiliza el término «sabotaje informático» -cyberpunking, vandalismo informático, vandalismo electrónico, cracking³⁸⁰o, para algún autor o en alguna ocasión, también hacking³⁸¹-, que hace referencia, en general, a todo el conjunto de conductas que dañan, impidiendo su correcto funcionamiento, elementos de naturaleza informática, quedando fuera del concepto, obviamente, conductas que se sirven del sistema para acceder a datos, redirigir conductas o introducir o distribuir información no deseada. Ahora bien, ni es necesaria la destrucción del objeto del ataque (en soporte o no), ni su desaparición total, ni un menoscabo funcional absoluto. Así, se ha descrito por algún autor el sabotaje como el conjunto de conductas de destrucción, inutilización o incapacitación de sistemas informáticos -englobando por supuesto en éstos los de carácter cibernético o telemático- o de datos o información contenida,

³⁸⁰DE ALFONSO LASO, «El hacking blanco. Una conducta ¿punible o impune?», pgs. 512 y ss., utiliza el término *cracker* para referirse al sujeto que se introduce en un sistema informático con el objetivo de realizar conductas de sabotaje informático; también, MATELLANES RODRÍGUEZ, «Vías para la tipificación del acceso ilegal a los sistemas informáticos», pg. 51. GÓMEZ MARTÍN, «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP)», pg. 3, o MORÓN LERMA, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, pgs. 40 y ss., sin embargo, reservan este término para aquellas conductas que neutralizan sistemas de protección de un *software* con el fin de realizar copias no autorizadas del mismo. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 204. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁸¹Utilizan este término RODRÍGUEZ/LASCURAÍN/ALONSO, «Derecho Penal e Internet», pg. 266, si bien el mismo se reserva por la mayoría de autores para conductas de intromisión en el sistema sin daño al mismo. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 204. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

*transferida o transmitida en los mismos, así como de sus funciones de procesamiento y tratamiento, ya se lleven a cabo las mismas mediante utilización de métodos lógicos, informáticos o telemáticos, ya mediante el abuso de los equipos físicos que permiten el acceso a dichos sistemas o datos*³⁸². (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 201-206)

Ahora, después de tener las definiciones de cada una de las actuaciones que pueden atacar, dañar y perjudicar los equipos informáticos vemos la posición de los doctrinantes frente a la adecuación típica, antijurídica y culpable, así:

*Pues bien, la definición de lo que se entiende por daño informático debe permitir incluir tanto la destrucción de sistemas informáticos completos como la de sus componentes concretos, ya sean equipos, datos, documentos o programas. Y, lo que conllevará no pocos problemas de tipificación, ha de abarcar tanto lo que es en sí la destrucción de tales elementos -o su inutilización- como la simple perturbación del funcionamiento del sistema completo o de alguno de sus componentes funcionales*³⁸³. No, en cambio, en nuestra opinión, el mero acceso no consentido a un sistema.

Dado que lo característico de los sistemas informáticos es su función de almacenamiento, procesamiento o transmisión de información, parece adecuado reservar el concepto de daño informático, al menos en este ámbito penal, para conductas que, de una u otra manera,

³⁸²Descriptivamente, ROVIRA DEL CANTO, *Delincuencia informática y fraudes informáticos*, pgs. 226 y ss. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 205. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁸³Véanse GONZÁLEZ RUS, «LOS ilícitos en la red (I): hackers, crackers, cyber-punks, sniffers, denegación de servicios y otros comportamientos semejantes», pg. 248; o MORÓN LERMA, «Derecho Penal y nuevas tecnologías: panorama actual y perspectivas futuras», pg. 114. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 205. En: *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas.

afecten a los elementos lógicos del sistema; ya, sin embargo, mediante la destrucción de todo el sistema informático, ya mediante la de alguno de sus componentes: programas, datos o documentos³⁸⁴, ya, a nuestro juicio, mediante la alteración de la funcionalidad del sistema por afectarse alguno de sus componentes físicos o lógicos que impide un uso plenamente satisfactorio del mismo. Justamente teniendo en cuenta que la destrucción de elementos físicos, aunque no necesariamente, lo normal será que implique el daño de elementos lógicos, seguramente de imposible recuperación, aunque no se realice con ese propósito, el término ha de permitir incluir ataques tanto a elementos físicos como a elementos lógicos del sistema³⁸⁵, en sus muy diversas modalidades, con independencia de dónde se ubiquen típicamente unos u otros.

Lo importante no es qué tipo de conducta se lleve a cabo, sino cuál es su consecuencia; y si ésta es la de alteración, desaparición, destrucción, inutilización o menoscabo de componentes del sistema que perjudiquen su funcionalidad (ya sea de sus aplicaciones, ya de sus programas, ya del acceso a sus datos), deberemos poder hablar de daño informático. (De La MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. 2010 P. 201-206)

³⁸⁴Así, por ejemplo, GONZÁLEZ RUS, «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicios y otros comportamientos semejantes», pgs. 248 y ss.; GUTIÉRREZ FRANCÉS, «Delincuencia económica e informática en el nuevo Código Penal», pgs. 291 y ss.; o ROMEO CASABONA, «Los delitos de daños en el ámbito informático», pg. 91. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 205. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

³⁸⁵Subraya MORILLAS FERNÁNDEZ, *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, pg. 108, que es incorrecto el uso del término sabotaje informático únicamente para los ataques a elementos lógicos de un sistema informático. Citado en: De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) P. 206. En: Derecho Penal Informático. Pamplona, España: Editorial Thomson Reuters. Civitas.

3.4.2. Legislación frente a los delitos informáticos, electrónicos y de las telecomunicaciones en Colombia

3.4.2.1. LEY COLOMBIANA SOBRE DELITOS ELECTRÓNICOS “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado- denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” (Ley 1273 del 5 de enero de 2009)

En Colombia se logra concretar la inclusión de “La información y los datos” dentro de los bienes jurídicos tutelados que protege el legislador a través de la Ley Penal. Es así como el 5 de enero del año 2009, por fin se sanciona la Ley 1273 de Delito Informático en Colombia, “Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”, siendo un avance significativo por cuanto reconoce la categoría de bien jurídico tutelado a la información y/o el dato, introduciendo su protección al ámbito penal, equiparando la legislación colombiana a los mayores desarrollos legislativos en la materia a nivel mundial, creando no sólo 9 tipos penales nuevos dentro del Código Penal Colombiano Ley 599 de 2000, para la protección de la información y los datos, sino también agregando como circunstancia de mayor punibilidad en el artículo 58 de la parte general del Código Penal, el numeral 17 que reza: “*Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos*”, circunstancia que permite un aumento de pena para la comisión

de cualquier tipo penal que se valga de dichos medios para vulnerar bienes jurídicos protegidos.

Los nuevos tipos penales y sus circunstancias de agravación punitiva son agrupados en un nuevo Título dentro del Código Penal, el Título VII Bis “De la protección de la información y de los datos”, que se encuentra dividido en dos capítulos, el primero denominado *“De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”* donde se penalizan con privación de la libertad y multa los delitos de: Acceso abusivo a un sistema informático (Art. 269A C.P.), Obstaculización ilegítima de sistema informático o red de telecomunicación (Art. 269B C.P.), Interceptación de datos informáticos (Art. 269C C.P.), Daño informático (Art. 269D C.P.), Uso de software malicioso (Art. 269E C.P.), Violación de datos personales (Art. 269F C.P.) y Suplantación de sitios web para capturar datos personales (Art. 269G C.P.). Y el segundo, denominado *“De los atentados informáticos y otras infracciones”* donde se penalizan, también con privación de la libertad y multa los siguientes delitos: Hurto por medios informáticos y semejantes (Art. 269I C.P.) y Transferencia no consentida de activos (Art. 269J C.P.).

La citada circunstancia de mayor punibilidad que agregó la Ley 1273 de 2009 (*“Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”*), al artículo 58 del Código penal en el numeral 17 ha permitido la persecución penal, investigación y juzgamiento de diferentes delitos, que aunque su naturaleza no sea de tipo informático, los medios que utilizan si lo son. Y en esta categoría recaen delitos contra el patrimonio económico, contra la libertad e integridad sexuales, contra los derechos de autor, contra la libertad individual y otras garantías. Lo que permite que en

Colombia, se reconozcan penal y judicialmente las dos categorías de delitos cibernéticos resultantes de los estudios de la Organización de las Naciones Unidas y el Consejo Europeo para delitos de alta tecnología: El primero, **Delito cibernético en sentido estricto** (“delitos informáticos”): todo compartimiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y de los datos procesados por ellos; y el segundo, **Delito cibernético en sentido lato** (“delito relacionado con computadoras”): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos”³⁸⁶. (RINCÓN RÍOS, J. 2010)

Otra característica importante de nuestra Ley de Delitos informáticos (*Ley 1273 de 2009 “Por medio del cual se crea el bien jurídico tutelado – denominado “De la protección de la información y de los datos”– y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*”), es que recogió plenamente las recomendaciones de la Convención de Budapest del año 2001, definiendo incluso competencias, radicándola en nuestro caso en cabeza de los Jueces penales municipales según el numeral 6° del artículo 37 de la Ley 906 de 2004 Código de Procedimiento Penal, superando de esta manera el debate entre delitos contra el Patrimonio Económico y delitos Informáticos, ratificando la Corte Suprema de Justicia en Proceso Radicado N° 34564 Sala de Casación Penal. M.P. José Leonidas Bustos Martínez, que cuando estos entran en contradicción, conocen los Jueces penales

³⁸⁶ Naciones Unidas, Décimo Congreso de las Naciones Unidas sobre la Prevención del Delito y Tratamiento del Delincuente, Viena, 10 al 17 de abril de 2000, Delitos relacionados con las redes informáticas, A/CONF.187/10, p. 5. http://www.unodc.org/pdf/crime/10_commission/resumed_session/14s.pdf, Página consultada marzo de 2007. RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

municipales sin importar la cuantía; simplemente la naturaleza digital del ilícito claramente determinada, por la clara competencia funcional determinada en la ley. (RINCÓN RÍOS, J. 2011)³⁸⁷

3.4.2.1.1. De los atentados contra la confidencialidad, la integridad y disponibilidad de los datos en los sistemas informáticos:

3.4.2.1.1.1. Acceso abusivo a un sistema informático. Artículo 269A de la Ley 599 de 2000 (Código Penal Colombiano). Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Es este un delito de mero peligro, donde el bien jurídico no es el sistema informático sino la información. Una analogía de esto se presenta cuando una persona ingresa sin autorización a un almacén que se encuentra cerrado; por el solo hecho del ingreso indebido ya se constituye en una conducta sancionable, protegiendo así la mercancía en él contenida. Continuando con la analogía, si la persona que ingresa está autorizada para dicho acceso, lo ilícito se presentaría no por el hecho de ingresar sino si efectivamente hace un uso abusivo o dañino del material protegido, conducta que recaería dentro

³⁸⁷ RINCÓN RÍOS J., (2011) De lo legislativo a lo jurisprudencial en materia de ciberdelincuencia en Colombia. Ponencia presentada en el XV Congreso Iberoamericano de Derecho e Informática. Buenos Aires, Argentina. 3 al 8 de octubre de 2011.

del tipo penal de *Daño en bien ajeno*. Lo cual es aplicable también a la información. (BOLAÑOS, F.A., MARTÍNEZ, J.E., 2004)

Lo ha tipificado la legislación Colombiana, así:

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

3.4.2.1.1.2. Obstaculización ilegítima de sistema informático o red de telecomunicación.
Artículo 269B de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Este tipo penal busca proteger la Disponibilidad del sistema informático o red de telecomunicación, pues la norma penal cumple con el Principio de Taxatividad y con la tipificación de esta conducta el legislador no busca penalizar los atentados contra la confidencialidad ni la privacidad del sistema informático, sino el atentado ilegítimo por medio del cual se obstaculice o impida su acceso, es decir, su disponibilidad.

El legislador colombiano en el artículo de la referencia lo estableció en los siguientes términos:

El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

3.4.2.1.1.3. Interceptación de datos informáticos.

Artículo 269C de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adionado por el artículo 1 de la Ley 1273 de 2009.

En este tipo penal es importante aclarar el concepto de datos y podemos decir que *“son aquellas informaciones, instrucciones o conceptos representados de manera convencional en una forma adecuada para el entendimiento humano o el procesamiento automático.”*(RINCÓN RÍOS, J. 2010)³⁸⁸

La tipificación en la Ley Penal Colombiana lo define en los siguientes términos:

³⁸⁸ RINCÓN RÍOS, J. (2010). Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

3.4.2.1.1.4. Daño Informático. Artículo 269D de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Se ha considerado que el delito de daños implica que se afecte la esencia o sustancia de la cosa, de manera que no sería constitutivos de delito los casos en los que, permaneciendo inalterada la estructura material del objeto, sólo se lesiona el valor de uso que la cosa tiene para el propietario. El sector doctrinal mayoritario, por el contrario, mantiene la existencia del delito cuando se priva al propietario del uso a que aparecía destinada la cosa dañada. (...)” (REYNA ALFARO, L.M. 2002:191)³⁸⁹

El artículo de la legislación citado ha tipificado este delito, así:

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de

³⁸⁹ REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores.

información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

3.4.2.1.1.5. Uso de software malicioso. Artículo 269E de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Definida esta conducta legalmente de la siguiente forma:

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Los sujetos activos de esta conducta son conocidos por los diferentes doctrinantes del Derecho Penal Informático como *Viruckers*. “La denominación referida proviene del apócope de las palabras virus y hacker, definiendo de esta manera a aquella persona que “*programa virus informáticos que se insertan dolosamente en sistemas informáticos, siendo una variante precisamente el que inserta un programa contaminado sin haber*

*intervenido en el diseño del programa destructor*³⁹⁰. Dicho accionar consiste en el ingreso doloso de un tercero a un sistema informático ajeno, con el objetivo de introducir “virus” y destruir, alterar y/o inutilizar la información contenida.

Existen dos tipos de virus (tratados anteriormente), los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar. Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores³⁹¹. Entendidos de esta manera según los efectos que ellos producen, diferenciándolo en dos categorías que a continuación se describen³⁹²:

“a) *Virus informáticos inofensivos*: como su definición lo expresa, producen efectos totalmente inofensivos en los programas. El único efecto que producen los virus informáticos inofensivos es un retardo o retraso en el funcionamiento del ordenador o computadora, o simples molestias.

a) *Virus informáticos nocivos o dañinos*: estos virus lógicamente son, en su mayoría, virus de segunda generación y pueden ser destructivos de software o destructivos de hardware. Es decir, pueden encriptarse haciendo más difícil su detección para los sistemas de seguridad y programas antivirus y, según se trate de un virus destructivo de

³⁹⁰ FILLIA, Leonardo César; MONTELEONE, Romna; NAGER, Horacio Santiago, SUEIRO, Carlos Christian, Análisis integrado de la criminalidad informática, Fabián J. Di Placido Editor, Bs. As., 2007. En cita a Marcelo Alfredo RIQUERT, p. 120. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 101.

³⁹¹ Disponible en <http://www.monografias.com/trabajos12/tsinnom/tsinnom2.shtml>. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 101.

³⁹² FILLIA, Leonardo César; MONTELEONE, Romna; NAGER, Horacio Santiago; SUEIRO, Carlos Christian, ob. cit., p. 105. Citado en: CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 101.

software de hardware, pueden efectuar operaciones tales como afectar el normal funcionamiento de los programas, borrar el disco rígido, duro o unidad “C”, contaminar archivos, afectar la BIOS, etc.” (CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., 2009:101.)

3.4.2.1.1.6. Violación de datos personales. Artículo 269F de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Frente a este ilícito se ha pronunciado ROVIRA DEL CANTO, en su obra *Delincuencia Informática y Fraudes Informáticos* (2002), quien define esta conducta ilícita como “Hacking informático”. Según el autor español, el término «hacking» tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje. Pese a lo anterior, su conducta es considerada lesiva, pues traspasa la «formal esfera de la privacidad y del secreto» o «la integridad del sistema informático afectado» (ROVIRA DEL CANTO, E. 2002:193)³⁹³

La tipificación legal de este delito es:

³⁹³ ROVIRA del CANTO, E. (2002) *Delincuencia Informática y fraudes informáticos*. Granada: Editorial Comares.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

3.4.2.1.1.7. Suplantación de sitios web para capturar datos personales. Artículo 269G de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Primero De los atentados contra la Confidencialidad, la Integridad y la Disponibilidad de los datos y de los sistemas informáticos. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

Phishing es un término utilizado en informática con el cual se denomina el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser información detallada sobre tarjetas de crédito, una contraseña u otra información bancaria. Quien lo practica es conocido con el nombre de phisher. El término phishing viene del inglés fishing que significa pesca, haciendo alusión al acto de pescar usuarios mediante carnadas o señuelos fabricados por los phisher cada vez más sofisticados y de este modo obtener información financiera y contraseñas. También se dice que el término phishing es la contracción de password harvesting fishing que significa: cosecha y pesca de contraseñas,

aunque esto probablemente es un acrónimo retroactivo³⁹⁴. Cierta doctrina define a estos agentes como aquellos piratas informáticos encargados de donar páginas web de instituciones bancarias o financieras, a fin de obtener mediante ellas las claves de los usuarios del sistema de transferencia electrónica de fondos³⁹⁵. (CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H. 2009:102)

Su contenido legal es el siguiente:

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

³⁹⁴ Disponible en <http://www.descargar-antivirus-gratis.com/phishing.php>. CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 102

³⁹⁵ FILLIA, Leonardo César; MONTELEONE, Romna; NAGER, Horacio Santiago; SUEIRO, Carlos Christian, ob. cit., p. 119. CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2009). Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus. P. 102

3.4.2.1.1.8. Circunstancias de agravación punitiva y Circunstancias de mayor punibilidad.

El legislador penal Colombiano en la redacción de la Ley 1273 de 2009 estableció en el artículo segundo, Capítulo Segundo, las circunstancias de agravación punitiva (artículo 269H del C.P.), aplicables a todos los tipos penales desarrollados en el Título VII BIS de la Ley 599 de 2000, Código Penal. Los agravantes aumentan la pena de las conductas descritas, de la mitad a las tres cuartas partes en las siguientes circunstancias:

- “1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.*
- 2. Por servidor público en ejercicio de sus funciones.*
- 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.*
- 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.*
- 5. Obteniendo provecho para sí o para un tercero.*
- 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.*
- 7. Utilizando como instrumento a un tercero de buena fe.*
- 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.”*

Otro aspecto relevante en la redacción de la Ley, es el artículo 2° del Capítulo Segundo, que modifica el artículo 58 de la Ley 599 de 2000, Código Penal, adicionando el numeral 17 a las circunstancias de mayor punibilidad, así:

“17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.”

Es importante tener en cuenta las diferencias dogmáticas entre las circunstancias de agravación punitiva y las circunstancias de mayor punibilidad, reconociendo a las primeras como *fundamentos reales modificadores de los límites de la pena*, y a las segundas como *fundamentos no modificadores de los límites de la pena*.

Se conocen como fundamentos reales modificadores de los límites de la pena todas aquellas circunstancias que afectan el hecho objeto de juzgamiento, previstas en la ley. Que tienen el efecto de variar los marcos punitivos, porque constituyen, en realidad, circunstancias específicas del hecho que hacen de él una forma especial de delincuencia para la cual el legislador ha reservado una sanción distinta de la del tipo básico.³⁹⁶ Lo anterior indica que se constituye un nuevo tipo penal con una pena diferente, por ejemplo quien incurra en el delito de *Intercepción de datos informáticos*, artículo 269C del C.P., pero realice la conducta *Con fines terroristas o generando riesgo para la seguridad o defensa nacional*, tal y como lo define el numeral 6 del artículo 269H, incurrirá en el delito de *Intercepción de datos informáticos agravado*, conducta para la cual el legislador ha determinado una pena distinta a la del tipo penal básico que es la *Intercepción de datos informáticos*.

³⁹⁶ GONZÁLEZ AMADO, I., 2006 P. 422. Citado en: NARANJO DUQUE, V., RINCÓN RÍOS, J. (2011). Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia. Cali, Colombia: Editorial Universidad Santiago de Cali. P. 126

Mientras que, los fundamentos no modificadores de los límites de la pena, como lo son las circunstancias de mayor punibilidad, comprenden todas aquellas que permiten al juez la individualización de la sanción que debe imponer al responsable de un hecho punible, sin que se alteren los límites mínimo o máximo de la pena correspondiente. Es decir, las circunstancias y condiciones que permiten al juez establecer, para cada caso concreto el quantum de pena que le corresponde a un específico sujeto y, por consiguiente, moverse entre mínimo y el máximo de la pena descrita en la ley, o sea, dentro del “ámbito punitivo de movilidad.”³⁹⁷ (NARANJO DUQUE, V., RINCÓN RÍOS, J. 2011:126)

3.4.2.1.2. De los atentados informáticos y otras infracciones

3.4.2.1.2.1. *Hurto por medios informáticos y semejantes.* Artículo 269I de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Segundo De los atentados informáticos y otras infracciones. Artículo adicionado por el artículo 1 de la Ley 1273 de 2009.

De igual forma a la doctrina penal española, como se estableció anteriormente, el delito de hurto a través de medios informáticos también es objeto de regulación en la legislación colombiana, *El objeto material del delito de hurto ha de ser un bien mueble, y por tal interpreta la doctrina un bien*

³⁹⁷ GONZÁLEZ AMADO, I., 2006 P. 424. Citado en: NARANJO DUQUE, V., RINCÓN RÍOS, J. (2011). Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia. Cali, Colombia: Editorial Universidad Santiago de Cali. P.126

corporal o material, aprehensible, tangible, entre otras cosas, porque sólo así es posible la sustracción. (MEZA VÁSQUEZ, B., 2009.)

Sin embargo, para el autor en cita anterior, como para nosotros es importante definir cual es la apreciación que se hace de los datos y la información como bienes, teniendo en cuenta su valor económico y si logran entrar a la esfera de dominio del sujeto activo, *Si se parte de la base de que en el uso de computadoras en realidad se trabaja con datos archivados y se maneja únicamente información, se suscita un grave problema a la hora de poder definir dicha información con las mismas características que tradicionalmente se exigen en el bien mueble a los efectos del delito de hurto. Es evidente que la información en sí misma no es algo tangible; esto no impide que pueda llegar a adquirir corporeidad en aquellos casos en los que se archiva o graba en medios tangibles como puede ser una cinta, un disco, disquete, etc., en cuyo caso no se plantearía problema alguno puesto que ya habría un concreto bien mueble corpóreo susceptible de ser aprehendido. Por tanto, en cuanto al concepto de bien mueble, se requiere una ampliación de los estrictos límites marcados por un concepto materialista de bien mueble. En base a esto, no habría inconveniente en admitir a la información computarizada como bien mueble y, por lo tanto, objeto material del delito de hurto, en cuanto sea susceptible de gozar de un determinado valor económico en el mercado. (MEZA VÁSQUEZ, B., 2009.)*

3.4.2.1.2.2. Transferencia no consentida de activos.

Artículo 269J de la Ley 599 de 2000. Título VII BIS De la Protección de la Información y de los Datos. Capítulo Segundo De los atentados informáticos y otras infracciones. Artículo

adicionado por el artículo 1 de la Ley 1273 de 2009.

La legislación penal colombiana, tipifica la transferencia no consentida de activos en el artículo 269J del Código Penal, estableciendo componentes normativos a este tipo y definiendo desde su redacción que implica el dolo como elemento subjetivo para su configuración, así:

“El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.”

La transferencia no consentida de activos regulada en Colombia puede explicarse para su correcta adecuación jurídica, en palabras de Francisco Javier Muñoz Cuesta, así:

En este tipo penal Debe concurrir una transferencia no consentida de cualquier activo patrimonial, lo que supone un cambio de titularidad de bienes de contenido económico que hace suyos con capacidad de disposición el sujeto activo de la acción delictiva, pudiendo tratarse de

la obtención de dinero contable o documental, un crédito o determinados servicios. En este sentido BAJO FERNÁNDEZ³⁹⁸ estima que activo patrimonial será apuntes contables, datos o valores patrimoniales y cosas físicas con valor económico. (...)

Es imprescindible la relación de causalidad entre la manipulación informática o el artificio semejante que motiva la transferencia no consentida y el perjuicio patrimonial causado a tercero, es decir que como consecuencia de la actividad que el sujeto activo lleva a cabo en el equipo o sistema informático, en la forma al principio descrita, se produce ese perjuicio. De producirse el perjuicio por causas diferentes a la alteración informática es evidente que no existiría el delito que tratamos, pudiendo aparecer otro contra el patrimonio o una estafa ordinaria si concurre el engaño bastante en forma tradicional de error en la persona que provoca un desplazamiento patrimonial, o simplemente tratarse de una conducta atípica al faltar uno de los elementos del tipo.

Destaca RODRÍGUEZ RAMOS³⁹⁹ que una vez realizada la manipulación o artificio que exige la figura delictiva lo relevante es que se produzca el perjuicio por el impulso de la actuación ilegítima previa ejecutada por el sujeto que pretende la transmisión de activos, relación por tanto mecánica entre la manipulación y la citada transmisión.

³⁹⁸ Citado en MUÑOZ CUESTA, F. J. 2009. Estafa informática, introducción de datos falsos en operaciones mercantiles vía internet que motivan transferencias de dinero no consentidas. Revista Arazandi Doctrinal Num. 1/2009. Tomado desde: [http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishi ng/Article.%20Estafa%20inform%20E0tica%20\(molt%20bo\).pdf](http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishi ng/Article.%20Estafa%20inform%20E0tica%20(molt%20bo).pdf) el 20 de enero de 2013.

³⁹⁹ Citado en MUÑOZ CUESTA, F. J. 2009. Estafa informática, introducción de datos falsos en operaciones mercantiles vía internet que motivan transferencias de dinero no consentidas. Revista Arazandi Doctrinal Num. 1/2009. Tomado desde: [http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishi ng/Article.%20Estafa%20inform%20E0tica%20\(molt%20bo\).pdf](http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishi ng/Article.%20Estafa%20inform%20E0tica%20(molt%20bo).pdf) el 20 de enero de 2013.

Por último es necesario que el sujeto actúe con ánimo de lucro, elemento subjetivo del injusto que se prevé expresamente en la redacción delictiva y que consiste, como en todos los delitos patrimoniales, en el propósito de obtener una utilidad o ventaja de la acción, sin perjuicio de la concurrencia del dolo genérico de conocimiento y voluntad de la ilicitud de la conducta que se lleva a cabo. (MUÑOZ CUESTA, J. 2008.)

3.4.3. Legislación frente a los delitos informáticos en Brasil

Las iniciativas legislativas en el Brasil, comenzaron su debate a finales de la década del 90, encaminadas inicialmente a modificar la Ley nº 7.646, de 18 de diciembre de 1987, sobre la garantía constitucional de la inviolabilidad de datos; de manera concreta la protección de la propiedad intelectual de programas por computador y su comercialización.

Así mismo, se promulgaron dos leyes más sobre seguridad de los datos del 16 julio de 1997, y el habeas data, 12 de noviembre de 1997⁵⁵⁰. Posteriormente, dos proyectos de ley fueron presentados, el Proyecto de Ley No. 01589 de 1999, sobre el comercio electrónico, la validez jurídica del documento electrónico y la firma digital.

De otro lado, fue aprobado por el Congreso el Proyecto de Ley nº 52, de 2000, sobre el comercio electrónico, el cual amplía la Ley Complementaria nº 95, de 1998. Posteriormente fue reformada la Constitución Política en su artículo 5º elevando a rango constitucional la protección de la información. (RINCÓN RÍOS, J. 2013)⁴⁰⁰

⁴⁰⁰ RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

3.4.4. Legislación Frente a los delitos informáticos en Argentina

Este país posee quizá la tradición legislativa más completa en el tema de la protección del dato informático, tanto a nivel normativo como de investigaciones, realizadas sobre el tema.

Ley / Decreto	Publicación
11723 - Propiedad Intelectual	30-sep-1933
25036 - Propiedad Intelectual (Modifica 11723)	14-oct-1998
Decreto 427- Firma digital en la administración pública.	1998
25326 - Habeas Data	02-nov-2000
Ley 863-Ejercicio del comercio electrónico responsable respecto del acceso a Internet de los menores de edad.	2002
Decreto 165/1994 - Propiedad Intelectual - Protección de Software	03-feb-1994
Ley 24624 – Presupuesto General de la Administración Nacional 1996	29-dic-1995
Decisión Administrativa 43/1996 - Uso de Tecnología.	07-may-1996
Ley 24766 - Ley de Confidencialidad	30-dic-1996
Ley 25506 - Firma Digital	14-dic-2001
Decreto 2628/2002 - Reglamentación Firma Digital	20-dic-2002
Disposición 5/2002 - Documentación Técnica de la Autoridad	06-may-2002
Certificante de la ONTI Artículo 5 – Constitución Nacional	24-jul-2006
Ley 26388- Delitos Informáticos	10-oct2006 ⁴⁰¹

RINCÓN RÍOS, J. (2013)⁴⁰²

3.4.5. Legislación frente a los delitos informáticos en Bolivia

Reglamentación para el registro de nombres de dominio, decreto supremo número 26624 proferido por el Consejo de Ministros del 14/05/2002, a través

⁴⁰¹ Seguridad de la información, “Delitos Informáticos-Legislación Alemania”, www.seguinfo.com.ar, última actualización 21/08/05, página web consultada en febrero de 2007. ⁵⁵³ Seguridad de la información, “Delitos informáticos-legislación Chile”, www.seguinfo.com.ar, última actualización 21/08/05, página web consultada febrero 2007.

⁴⁰² RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

del cual se reglamenta el ordenamiento de redes y sistemas a partir del sector estatal. No se encontró ningún desarrollo legislativo que contemplara el Comercio Electrónico o la penalización de los delitos que atentan contra el bien jurídico de la información; de otro lado, se encuentra el Decreto Transparencia y Acceso a la Información Gubernamental Decreto Supremo No. 27329 del 31 de enero de 2004. (RINCÓN RÍOS, J. 2013)⁴⁰³

3.4.6. Legislación frente a los delitos informáticos en Chile

Documentos Electrónicos, Ley 19799 de Firma Electrónica del 12 de abril de 2002; los Servicios de Certificación de la Firma Electrónica y la Ley 19.223 de 1993 contra delitos informáticos; en ella se penalizan ciertas conductas como el *hacking*. Vale la pena precisar que “Chile fue el primer país latinoamericano en sancionar una ley contra Delitos Informáticos.”⁵⁵³ Ley 19223 de 1993, De otro lado encontramos la ley 19628 sobre Protección de Datos de Carácter Personal (1999), la Modificación de la Ley de Protección de Datos de Carácter Personal (2002) y la Ley contra Pornografía Infantil (2004)⁴⁰⁴. (RINCÓN RÍOS, J. 2013)⁴⁰⁵

4. ALCANCE DE LA CONVENCIÓN DE BUDAPEST, DEL DERECHO INTERNACIONAL HUMANITARIO Y LA COMPETENCIA Y JURISDICCIÓN DE LA CORTE PENAL INTERNACIONAL FRENTE A LOS DELITOS INFORMÁTICOS ELECTRÓNICOS Y DE LAS TELECOMUNICACIONES.

⁴⁰³ RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

⁴⁰⁴ Cfr. Seguridad de la información, “Legislación referente a seguridad de la información”, www.segu-info.com.ar, última actualización 21/08/05, página web consultada febrero 2007. Citado en: Rincón Ríos, J. 2013. Fraude en la Contratación electrónica internacional. Biblioteca de Tesis doctorales. Ibáñez: Bogotá.

⁴⁰⁵ RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

4.1. Derecho Penal Internacional y sus fuentes

En este momento investigativo debemos iniciar el desarrollo de este capítulo de forma deductiva, partiendo del concepto general de Derecho Penal Internacional, y para este propósito hemos tomado como referente al autor Alemán Kai Ambos, cuando manifiesta *Por derecho penal internacional ("Völkerstrafrecht")*⁴⁰⁶ se entiende, tradicionalmente, el conjunto de todas las normas de derecho internacional que establecen consecuencias jurídico-penales.⁴⁰⁷ Adicionalmente el autor en cita propone frente a la definición de esta rama del derecho que *Se trata de una combinación de principios de derecho penal y de derecho internacional.*⁴⁰⁸ AMBOS, K. (2006: 33).

⁴⁰⁶Sobre el concepto, utilizado por primera vez por *Beling*, cfr. *Jesche.k/Weigend*, AT (1996), p. 119, nota 4. Decididamente en favor del concepto *Jescheck*, *Verantwortlichkeit* (1952), p. 8; *Makarov*, FS Kern (1968), p. 253; en contra *Oehler*, *InternationalesStrafrecht* (1983), p. 606; cfr. también *Bremer*, *Strafverfolgung* (1999), p. 44 ss.; *Ahlbrecht*, *Geschichte* (1999), p. 9; *Bruer-Schafer*, *Strafgerichtshof* (2001), p. 26 ss. En general, sobre los méritos de *Jescheck* y de la terminología *Triffterer*, FS *JescheckII* (1985), p. 1478 ss.; *el mismo*, ÖJZ 1996, 326 s.; *el mismo*, GS Zipf (1999), p. 500 s. Sobre la delimitación con el concepto de "internationalesStrafrecht" (derecho penal internacional) también ya *Ambos*, en: *Arnold/Burkhardt/Gropp/Koch* (editores), *Grenzüberschreitungen* (1995), p. 250. Sobre la evolución del derecho penal internacional cfr. *Ahlbrecht*, *Geschichte* (1999), p. 19 ss. y passim, *Bruer-Schafer*, *Strafgerichtshof* (2001), p. 35 ss.; *Balboni*, in: *Illuminati et al.* (eds.), *Crimini* (2000), p. 1 ss.; *Bassiouni*, *Introduction* (2003), p. 23 ss., 393 ss. Desde la perspectiva latinoamericana con interesantes referencias, especialmente a los trabajos de *Jiménez de AsúaCarnevali*, RUCN 10 (2003), p. 32 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 34

⁴⁰⁷Cfr., para mayores detalles, *Triffterer*, *Untersuchungen* (1966), p. 34: "derecho penal internacional en sentido formal es el conjunto de todas las normas de naturaleza penal del derecho internacional, que conectan a una conducta determinada —crímenes internacionales— ciertas consecuencias típicamente reservadas al derecho penal y que, como tales, son aplicables directamente". Crít. sobre el concepto y su fundamentación *Köhler*, *Jb. RechtundEthik* 11 (2003), 443 ss. Respecto del concepto de crímenes internacionales, cfr. *Bremer*, *Strafverfolgung* (1999), p. 68 ss.; *Ahlbrecht*, *Geschichte* (1999), p. 8 ss. (9). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 34

⁴⁰⁸Cfr. también *van Sliedregt*, *Responsibility* (2003), p. 4: "meeting of two worlds". Sobre los varios componentes del d.p.i. ver *Bassiouni*, *Introduction* (2003), p. 1 ss. que lo califica como ".si// generis system" (p.53). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 34

Sabemos que el objetivo del derecho penal, en general, bajo su concepto de aplicabilidad bajo última ratio lo que busca, dentro del esquema dogmático finalista, es generar en su fase final un juicio de reproche y responsabilidad a los sujetos activos de la conducta, así mismo lo plante Ambos cuando establece que *la idea central de la responsabilidad individual⁴⁰⁹ y de la reprochabilidad de una determinada conducta (macrocriminal) proviene “del derecho penal, AMBOS, K. (2006:34). Ahora es necesario unir este concepto al de derecho internacional, teniendo entonces que las clásicas figuras penales (de Núremberg),⁴¹⁰ en su calidad de normas internacionales, se deben clasificar formalmente como derecho internacional, sometiendo de este modo la conducta en cuestión a una punibilidad autónoma de derecho internacional (principio de la responsabilidad penal directa del individuo según el derecho internacional). AMBOS, K. (2006:34).*

Tenemos entonces que por derecho penal internacional encontramos la rama del derecho que busca determinar la responsabilidad a través de un juicio de reproche a los sujetos que cometan conductas macrocriminales, es decir, que sobrepasan los límites territoriales, lo que le entrega el componente de internacional a este concepto.

⁴⁰⁹Sobre su reconocimiento ya en Núremberg ver p. 84 ss. vers. al. y Ambos, en *McDonald/Swaak-Goldman*, Int. Criminal Law, t. 1 (2000), p. 1 ss. = RP 7 (2001). R 5 ss. Ver también *Bassiouni*, Introduction (2003), p. 12, 47, 59, 64 ss. (106). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 34

⁴¹⁰Cfr. el art. 6 del EIMT (anexo al Acuerdo de Londres de las cuatro potencias del 8 de agosto de 1945): crímenes contra la paz, crímenes de guerra, crímenes contra la humanidad. Cfr., con más detalles, § 2 I. 1. (p. 81 ss.) vers. al. Sobre el desarrollo histórico *Ambos*, CLF 2003, p. 226 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 35

En la evolución del Derecho Penal Internacional, encontramos que *los desarrollos más recientes que culminaron en la aprobación del ECPI⁴¹¹ no sólo consolidan al derecho penal internacional como sistema de derecho penal de la comunidad internacional,⁴¹² sino que amplían su ámbito de regulación más allá de sus fundamentos jurídico-materiales a otras zonas accesorias del derecho penal (derecho sancionatorio, ejecución penal, cooperación internacional y asistencia judicial), al derecho procesal penal y a cuestiones de organización judicial.* AMBOS, K. (2006:35).

Con los preceptos anteriores vemos como el derecho penal internacional ha evolucionado hasta el punto de convertirse en todo un sistema que permite la investigación, juzgamiento y sanción de conductas delictivas en el plano internacional.

El gobierno federal Alemán así lo estableció:

Como acertadamente se ha expresado en el memorándum del gobierno federal alemán, con ello se ha conseguido "reunir y desarrollar en una obra de codificación unificada el derecho penal internacional, teniendo en consideración los diferentes sistemas de derecho penal, con sus respectivas tradiciones, de los Estados miembros de las Naciones Unidas".⁴¹³ Nos encontramos, por ello, no sólo frente a un

⁴¹¹Cfr. supra, nota 3. Sobre el estado de las ratificaciones, cfr. § 13 (síntesis), nota 34. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 35

⁴¹²Cfr. *Triffterer*, Politische Studien, Sonderheft 1/1995, 38. Ver también *Bassiouni*, en: AIDP (ed.), *International Criminal Law* (2004), p. 79 ss. (81) promoviendo un "system of international criminal justice" construido con base en los sistemas nacionales y el supranacional. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 35

⁴¹³BR-Drs. 716/99, p. 99. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 35

ordenamiento jurídico-penal internacional nuevo y autónomo, sino también frente a uno amplio, del cual la parte general que aquí se estudia constituye solamente un pequeño fragmento, si bien desde el punto de vista dogmático probablemente el más importante. AMBOS, K. (2006:35).

Con el establecimiento del Estatuto de la Corte Internacional de Justicia y el Estatuto de la Corte Penal Internacional, el derecho penal internacional no ha perdido su categoría de derecho público, razón por la cual debe componerse de principios y derechos fundamentales para la interpretación y aplicación de su desarrollo normativo.

El autor en cita lo planteado de la siguiente forma:

Puesto que el derecho penal internacional es al mismo tiempo parte del derecho internacional público formal, puede originarse, básicamente, a través de la celebración de convenciones multilaterales por los Estados interesados (cfr. art. 38 (I)(a), ECIJ) o a través de la formación de derecho consuetudinario o principios generales del derecho (cfr. art 38 (I)(b) y (c), ECIJ).⁴¹⁴ El derecho consuetudinario y los principios generales del derecho son, por cierto, difíciles de identificar, dado que se trata aquí de derecho internacional no escrito. Sin embargo, en tanto falten las convenciones correspondientes, estas fuentes del derecho deben servir como punto de partida constructivo para la formación de

⁴¹⁴Sobre el reconocimiento de la teoría de las fuentes del derecho internacional en el derecho penal internacional, ya *Triffterer*, *Untersuchungen* (1966), p. 35 ss.; también *el mismo*, FS JescheckII (1985), p. 1486 (remitiéndose a Jescheck); *el mismo*, ÓJZ 1996, 327 ss.; *el mismo*, en: Lüderssen (editor), *KriminalpolitikIII* (1998), p. 314 ss.; recientemente también *Krefi*, ZStW 1999, 599 s.; *Simma/Paulus*, en: Ascensio/Decaux/Pellet, *Droitinternational penal* (2000), p. 55 s.; *van Sliedregt*, *Responsibility* (2003), p. 6 ss.; *Bassiouni*, *Introduction* (2003), p. 8 ss., 51.Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 35

normas de derecho penal internacional; tampoco con el ECPI estas fuentes han perdido completamente su importancia, pues éste deja abiertos algunos ámbitos de regulación. AMBOS, K. (2006:35).

“De este modo, el art 21 (l)(b),⁴¹⁵ que establece el derecho aplicable, remite expresamente a los "principios y normas de derecho internacional" ("principles and rules of international law"), incluyendo como derecho aplicable de la futura CPI, entre otras cosas, a la costumbre internacional y a los principios generales de derecho en el sentido del art 38 ECJ.⁴¹⁶ AMBOS, K. (2006:35).

En la aplicación del derecho penal internacional es indispensable tener claridad sobre los criterios de interpretación y aplicación normativa, puesto que los acuerdos firmados por los Estados no implican la homogeneidad de sus legislaciones penales, razón por la cual la actuación de los tribunales penales internacionales debe estar ligada a la aplicación de las fuentes y principios generales del derecho penal y del derecho internacional.

Así se ha establecido en la obra citada:

En lo que respecta en particular a las fuentes del derecho penal internacional, la fundamentación en el derecho consuetudinario de normas de derecho penal internacional plantea especiales dificultades en un doble sentido. Desde la óptica del derecho penal el principio del nullum crimen parece excluir la existencia de tipos penales no escritos

⁴¹⁵ Las disposiciones sin indicación de fuente pertenecen al ECPI. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

⁴¹⁶Cfr. McAuliffe de Guzman, en: Triffterer (ed.), Commentary (1999), art. 21, nm. 11 ss.; Simma/ Paulus, en: Ascensio/Dcaux/Pellet, Droitinternational penal (2000), p. 56 s.; Schabas, Introduction (2004), p. 91 s. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

*fundados en la costumbre internacional.⁴¹⁷ Sin embargo, conforme a los arts. 15 (2), PIDCP, 11 (2), DUDH y 7 (2), CEDH una conducta puede ser sancionada, si ella era punible "según los principios generales de derecho reconocidos por la comunidad internacional".⁴¹⁸ Aquí, el concepto "principios de derecho" no se tiene que entender en el sentido del art. 38 (I)(c), ECtJ, sino en el de las reglas de derecho consuetudinario internacional desarrolladas sobre la base del derecho de Núremberg,⁴¹⁹ por lo cual la regla aplicada debe tener "sin duda" el carácter de costumbre internacional.⁴²⁰ La "desformalización" que esto implica o bien la carga normativa del principio *nullum crimen* se mostrará en el curso de la investigación aún en otros lugares.⁴²¹ Desde luego, ella ha perdido importancia con la codificación de los crímenes nucleares de derecho penal internacional en los arts. 5 a 8 y con la*

⁴¹⁷Cfr. también *Triffterer*, Untersuchungen (1966), p. 35 ss.; *el mismo*, en: Hankel/Stuby, Strafgerichte (1995), p. 218 s.; *el mismo*, en: Lüderssen (editor), Kriminalpolitik III (1998), p. 315 s. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

⁴¹⁸Cfr. ya *Ambos*, StV 1997, p. 39 ss.; recientemente *Broomhall*, en *Triffterer* (ed.), Commentary (1999), art. 22, nm. 25; *Bremer*, Strafverfolgung (1999), p. 60 ss. Por el contrario, el art. 9 de la CADH no contiene esta excepción. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

⁴¹⁹Cfr. *Simma/Paulus*, en: Ascencio/Dcaux/Pellet, Droit international penal (2000), p. 60, 64; también, *Caracciolo*, en: Lattanzi/Schabas (eds.), Essays (1999), p. 227. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

⁴²⁰Cfr. UN, Report of the Secretary General (1993), para. 34: "[...] rules [...] beyond any doubt part of customary law [...]". Cfr. también *Triffterer*, GS Zipf (1999), p. 502 s., quien con acierto señala que es admisible que el derecho consuetudinario fundamente y agrave la pena; en cambio, los principios generales de derecho no podrían fundamentar nuevas figuras penales, "porque a través de principios no se pueden establecer descripciones concretas de los comportamientos punibles" (ibidem, p. 505); del mismo modo *Simma/Paulus*, en: Ascencio/Dcaux/Pellet, Droit international penal (2000), p. 64. En diferente sentido, sin embargo, *Triffterer*, Untersuchungen (1966), p. 127 s.: "[...] que todas las fuentes del derecho penal internacional entran en consideración como posibilidades de creación de normas penales internacionales" (resaltado por el autor). Esto incluye a los principios generales de derecho. Diferenciando *Triffterer*, ÖJZ 1996, 328: "a través de principios generales de derecho reconocidos se pueden describir en un modo suficientemente determinado, sin embargo, solamente aquellos hechos cuya punibilidad pertenece al núcleo del derecho penal [...]" (resaltado por el autor). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 36

⁴²¹ Cfr. resumidamente, infra § 2 III. 1., § 6 II. 2. y III. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

aprobación adicional de los llamados "elementos de los crímenes" ("elements of crimes", de modo abreviado: "elementos") en virtud del art. 9.⁴²² AMBOS, K. (2006:37).

Quiere decir lo anterior, que en el desarrollo del derecho penal internacional y su aplicación, la fase de la adecuación típica de una conducta sobrepasa los planteamientos del derecho penal en el esquema romano germánico, adecuándose a las reglas del derecho consuetudinario por la necesidad de unificar la persecución de conductas macrocriminales para diferentes Estados, de forma que una conducta se considera delito cuando atenta los preceptos y principios generales del derecho penal internacional.

Esta situación genera la necesidad de establecer un derecho consuetudinario internacional y que ha sido ya planteada por Ambos, así:

Desde la óptica del derecho internacional se presenta el problema de que la praxis de los Estados (repetitiofacti), necesaria junto con un convencimiento jurídico general (opinio iuris) para el nacimiento del derecho consuetudinario internacional, difícilmente se pueda fundamentar de cara a la amplia extensión de la impunidad de las

⁴²²Los elementos de los crímenes fueron aprobados provisoriamente en la quinta sesión de la Preparatory Commission (Prep-Commis) en Nueva York (12.6-30.6.2000) (PCNICC/2000/INF/3/Add. 2) y definitivamente por la Asamblea de Estados Partes en su primera reunión en septiembre de 2003 (ICC-ASP/ 1/3, cfr. <www.un.org/law/icc>). Ellos no poseen un efecto vinculante directo, sino que solamente deben "ayudar" a la Corte en la interpretación, debiendo ésta examinar su compatibilidad con el ECPI (cfr. *Gadirov*, en: Triffterer (ed.), Commentary (1999), art. 9, nm. 30; *Dórmann/Krefi*, HuV 1999, 203; *Lindenmann*, HuV 1999, 213; *von Hebel/Robinson*, en: Lee [ed.], ICC [1999], p. 87 s.; *Robinson/von Hebel*, YIHL, 1999, 206; *Caracciolo*, en: Lattanzi/Schabas [eds.], Essays [1999], p. 226; *Schabas*, Genocide [2000], p. 173; *Triffterer*, FS Roxin [2001], p. 1416, 1425; *Lagodny*, ZStW 2001, 807; *Boot*, Crimen [2002], p. 35 s.). Cfr. para un panorama, *Ambos*, NJW 2001, 405 ss.; detalladamente *Rückert/Witschel/Dórmann*, en: Fischer/RreB/Lüder (eds.), Prosecution (2001), p. 59 ss. y 95 ss.; *Lee* (ed.), ICC (2001), p. 3 ss.; crít. *Hunt*, JICJ 2004, p. 59 ss., 65 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

severas violaciones a los derechos humanos.⁴²³ Este problema puede ser atendido mediante una más fuerte acentuación de los principios generales del derecho. Ante todo, los principios generales del derecho existentes pueden ser traídos en consideración para la verificación o falsación de las reglas de derecho consuetudinario internacional en formación y, en consecuencia, aún no consolidadas. En caso de verificación de la regla de derecho consuetudinario internacional correspondiente se fundamentaría, por medio de una semejante solución de combinación, una nueva regla de derecho internacional.⁴²⁴ Con esto se desarrollaría un principio general del derecho —de modo absolutamente tradicional— a partir del derecho nacional con base en investigaciones de derecho comparado, en cierto modo como "general principles of law derived [...] from national laws of legal systems of the world [...]" (art. 38 (l)(c), ECIJ).⁴²⁵ Además, según la opinión preponderante en la actualidad, los principios generales del derecho se pueden fundamentar,⁴²⁶ también, en una valoración de conjunto del softlaw⁴²⁷ internacional, como una especie de "opinio iuris

⁴²³Respecto de la "missionary writing" y de las "words" en lugar de "deeds" en este contexto *Simma*, en: Academy of European Law (ed.), *Collected Courses IV* (1995), p. 216 ss. Sobre el derecho consuetudinario europeo *Bleckmann*, *VwZ* 1993, 827. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

⁴²⁴Cfr. *Simma/Paulus*, *AJIL* 1999, 313 (en cuanto a la punición de crímenes de guerra en un conflicto no internacional); también *Krefl*, *ZStW* 1999, 613 ss. (en cuanto al reconocimiento en derecho penal internacional del estado de necesidad por coacción). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

⁴²⁵Cfr. en general *Krefl*, *ZStW* 1999, 608 ss., con otras referencias; también *Lahti*, en: AIDP (ed.), *International Criminal Law*, 2004, p. 345 s. Sobre los principios generales del derecho en el derecho de la Comunidad Europea, cfr., en este sentido, art. 6 (2), TUE, así como *Bleckmann*, *NVwZ* 1993, 825 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

⁴²⁶Sobre todo esto *Ambos*, *AVR* 1999, 332 ss., con otras referencias Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 37

⁴²⁷Dentro de este concepto entran, por ejemplo, las decisiones de los organismos internacionales no jurisdiccionales, los demostrables esfuerzos de codificación, las declaraciones de las conferencias diplomáticas, etc. Sobre el concepto: *Verdross/Simma*, *Völkerrecht* (1984), § 540 ss., 654 ss.; sobre el "softlaw" de los derechos humanos *Simma*, en: Academy of European Law (ed.), *Collected Courses IV* (1995), p. 233 ss.; *Simma/Paulus*,

without concordant state practice".⁴²⁸ En esa dirección argumenta en definitiva también el Tribunal para la antigua Yugoslavia (ICTY) cuando funda una prohibición fundamental de represalias en caso de ataques a civiles en el campo de batalla, esencialmente, en las "*demands of humanity and the dictates of public conscience, as manifested in opinio necessitatis*".⁴²⁹ Tal comprensión moderna de los principios generales del derecho conduce a una asimilación del derecho consuetudinario internacional con los principios generales del derecho, en el sentido de trascendentes "*principios y normas del derecho internacional*" ("*principles and rules of international law*") según el art. 21 (l)(b).⁴³⁰ El derecho consuetudinario internacional es, con esto, parte de las "*normas*" ("*rules*");⁴³¹ los principios generales del derecho contienen una doble función.⁴³² Por un lado, como reglas supranacionales

en: Ascensio/Dcaux/Pellet, *Droit international penal* (2000), p. 66. Citado en: AMBOS, K. (2006). *La parte general del Derecho Penal Internacional*. Bogotá D.C.: Editorial Temis. P. 37

⁴²⁸ *Simma*, en: Academy of European Law (ed.), *Collected Courses IV* (1995), p. 225. En similar sentido Bassiouni, Mich JIL 1990, 768 s.: "when a custom is not evidenced by [...] practice, or when States express *opinio iuris* without any supportive practice". Uno de los defensores más destacados de un derecho consuetudinario internacional fundado fuertemente en la "*opinio iuris*" es probablemente *Theodor Meron* (AJIL 1995, 554 ss. y AJIL 1996, 238 ss.). Sobre principios generales en el derecho consuetudinario cfr. también *Weigend*, en: A1DP (ed.), *International Criminal Law* (2004), p. 319 ss. Citado en: AMBOS, K. (2006). *La parte general del Derecho Penal Internacional*. Bogotá D.C.: Editorial Temis. P. 38.

⁴²⁹ *Prosecutor v. Kupreskic et al.*, Judgment 14.1.2000 (IT-95-16-T), para. 527 ss. (533, resaltado en el original); sobre esto, con más detalles p. 305 ss. vers. al. De esta manera, la Sala quiere fundamentar una regla de *derecho consuetudinario internacional* y renuncia, de forma dudosa, al elemento constitutivo de la praxis de los Estados (crít. sobre esa tendencia ya *Ambos*, AVR 1999, 328 ss.). Citado en: AMBOS, K. (2006). *La parte general del Derecho Penal Internacional*. Bogotá D.C.: Editorial Temis. P. 38.

⁴³⁰ Cfr. también *Simma/Paulus*, en: Ascensio/Dcaux/Pellet, *Droit international penal* (2000), p. 61: "Ce n'est pas par hasard que la coutume et les principes généraux de droit semblent se rapprocher"; Citado en: AMBOS, K. (2006). *La parte general del Derecho Penal Internacional*. Bogotá D.C.: Editorial Temis. P. 38.

⁴³¹ Cfr. *McAuliffe de Guzman*, en: Triffterer (ed.), *Commentary* (1999), art. 21, nm. 14. Citado en: AMBOS, K. (2006). *La parte general del Derecho Penal Internacional*. Bogotá D.C.: Editorial Temis. P. 38.

⁴³² Cfr. también *Simma/Paulus*, en: Ascensio/Dcaux/Pellet, *Droit international penal* (2000), p. 62 ss.; similar *Caracciolo*, en: Lattanzi/Schabas (eds.), *Essays* (1999), p. 228 Asimismo, en el derecho comunitario europeo los principios generales de derecho de la Comunidad, de un lado, y los principios generales de derecho de los Estados miembros, del otro, cfr. *Krück*, en: von der Groeben/Thiesing/Ehlermann (editores), *ELVEG-Vertrag* (1997), art. 164, nm. 22 ss.

originarias ellos colaborarían a la formación de la costumbre internacional o —según una comprensión moderna— a la de reglas de derecho internacional. Por otro lado, como principios generales del derecho en sentido tradicional ellos representarían una fuente autónoma. En este sentido, aunque de acuerdo con el art. 21 (1) (c) deben ser aplicados sólo subsidiariamente,⁴³³ ellos asumen sin embargo una considerable importancia⁴³⁴ en atención del estado aún rudimentario del derecho penal internacional escrito y no escrito,⁴³⁵ especialmente en su parte general. AMBOS, K. (2006:38).

Es necesario dentro de la estructuración del derecho penal internacional comparado la fundamentación de los principios, pues son los que permiten la unificación de las legislaciones firmantes de los tratados y bajo sus márgenes se regulará la eventual responsabilidad de los asociados de cada Estado, razón por la que cada debe velar por la protección de los derechos fundamentales de los mismo, por esta razón debemos enfatizar la importancia del derecho penal comparado, tal y como lo establece el autor en cita, así:

De este modo, se evidencia a la vez el importante rol que le cabe al derecho penal comparado: éste colabora con la fundamentación de principios generales del derecho en sentido tradicional, permitiendo

Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 38.

⁴³³Cfr. *McAuliffe de Guzman*, en: Triffterer (ed.), *Commentary* (1999), art. 21, nm. 2 ss., 15 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 38.

⁴³⁴Similar *McAuliffe de Guzman*, en: Triffterer (ed.), *Commentary* (1999), art. 21, nm. 17; *Schabas*, *Introduction* (2004), p. 92; *Lagodny*, *ZStW* 2001, 817; *Vest*, *Genozid* (2002), p. 29; *Fronza*, en Papa (director), *Orizonti* (2003), p. 14 ss.; *Fronza/Guillou*, en DelmasMarty/Muir Watt/Ruiz Fabri, *Variations* (2002), p. 286 ss.; *los mismos* en Chiavario (editor), *La justice pénale internationale* (2003), p. 38 ss. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 38.

⁴³⁵Cfr., por ejemplo, *Cassese*, citado según McDonald/Swaak-Goldmann, en: ellos mismos (eds.), *Int.Crim.L. I* (2000), p. XIII: El derecho penal internacional sería "still quite rudimentary" y carecería de "thespecificity of most municipal criminal law".Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 38

deducir de las regulaciones concretas de los derechos nacionales un principio común.⁴³⁶ Desde luego, no se puede partir aquí solamente del propio sistema nacional del hecho punible, convirtiendo, por ejemplo — en el sentido del método tradicional, normativo-descriptivo, del derecho comparado—, el punto de vista dogmático propio en el punto de partida y centro de las consideraciones de derecho comparado.⁴³⁷ El peligro de este método es evidente: si se parte de un punto de vista semejante, basado en el derecho propio, los conocimientos logrados con motivo de la comparación jurídica no se diferenciarían radicalmente de éste y se prejuzgaría su valoración jurídico-política. Por ello, se ha de preferir un moderno método funcional, el cual se oriente —en el sentido de una orientación empírica— a los problemas materiales hallables en un orden jurídico determinado y que se interroga, en la solución de estos problemas, por el rol y la función de los institutos jurídicos existentes, para posibilitar, de esta manera, una comparación —sin prejuicios conceptuales ni dogmáticos— con los institutos jurídicos funcionalmente correspondientes en ordenamientos jurídicos extranjeros.⁴³⁸ Si

⁴³⁶Sobre la importancia para el derecho penal internacional de la comparación (legislativa) de derecho penal, también Eser, FS Kaiser (1998), p. 1506, 1508 s., 1514; Delmas-Marty, JICJ 2003, p. 13 ss.

(18 ss.) enfatizando la "hybridization". Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 39.

⁴³⁷Cfr. en este sentido aún Jescheck, Entwicklung (1955), p. 36 ss. (37 s., 40 ss.): Partiendo de un *punto de vista* político criminal o dogmático (propio) (primer nivel) él pretende *interpretar* el derecho extranjero (exégesis, segundo nivel), luego *sistematizarlo* (tercer nivel) y finalmente *valorarlo* jurídico-políticamente (cuarto nivel). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 39.

⁴³⁸Sobre el principio fundamental de la funcionalidad en el derecho comparado Kótz, RabelsZ 1990, 209 s.; Zweigert/Kótz, Rechtsvergleichung (1996), p. 33 ss.; Eser, FS Kaiser (1998), p. 1521; también Weigend, ZStW 1993, 787 s., Vogel, JZ 1995, 337 s. (sin embargo, crít. sobre este autor, infra nota 37 y 129). Cfr. también Perron, ZStW 1997, 285 ss., 296 ss., con otras referencias, quien en el marco de su proyecto de investigación "Allgemeiner strafrechtlicher Strukturvergleich" ("Comparación de estructuras de parte general del derecho penal") desarrollado en el Instituto Max Planck para Derecho Penal Extranjero e Internacional de Friburgo persigue, sobre la base del análisis de casos, un enfoque fuertemente orientado en consideraciones jurídico-fácticas y, con ello, espera unir un método empírico con uno normativo (Cfr. <www.iuscrim.mpg.de/de/forsch/straf/projekte/perron.html.de>; también Eser, FSKaiser

bien nunca se podrá evitar completamente la parcialidad del derecho penal nacional,⁴³⁹ al menos este método ofrece la chance de descubrir, "libre de los conceptos de sistema del ordenamiento jurídico propio",⁴⁴⁰ una solución materialmente adecuada para un problema jurídico determinado. Para no actuar de modo simplemente funcional y desvinculado de las decisiones de valor de derechos fundamentales de los sistemas jurídicos más importantes,⁴⁴¹ se propone utilizar el conocido principio de la comparación jurídica valorativa proveniente del derecho comunitario europeo.⁴⁴² Si allí con este principio se trata —desde el punto de vista de los derechos fundamentales— de una maximización de la protección de los derechos fundamentales,⁴⁴³ en el plano del derecho penal internacional se podrá hablar de una maximización de la protección de los derechos humanos. AMBOS, K. (2006:40).

[1998], p. 1519 s.). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 39.

⁴³⁹Cfr. *Weigend*, RIDP 1981, 500: "[...] even after discarding all benign comparativist rhetoric aside, one will find that jurists everywhere are likely to regard their own system of justice not necessarily perfect, but as better than the rest". Similar, también, *Bogdan*, NordicJIL 1977, 49; *Eser*, en: Bassiouni (ed.), Commentaries (1993), p. 44. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 39.

⁴⁴⁰*Zweigert/Kötz*, Rechtsvergleichung (1996), p. 33. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 39.

⁴⁴¹En este peligro se encuentra la "reserva de función" de *Vogel* (JZ 1995, 336 ss., 336), cuando él se orienta completamente —en el sentido de su funcionalidad "jurídico-externa"— a las exigencias o al funcionar del mercado común (crít. también *Weigend*, FS Roxin [2001], p. 1381 s.). Aquí existe una patente cercanía con el "puro" funcionalismo de impronta jakobsiana (infra, nota 129). De todos modos se le debe conceder a *Vogel* que *in abstracto* difícilmente se puedan proponer medidas de contenido más preciso que las que él ha desarrollado (338 ss.). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40.

⁴⁴²El concepto se remonta a *Zweigert*, *RabelsZ* 1964, 611: "principio general del derecho es [...], lo que se presenta como la mejor solución, luego de un análisis crítico de las soluciones que resultan de una mirada al derecho comparado". El concepto fue recogido por el fiscal general *Roemer* por primera vez en la causa *Stauder* (TEDH, Slg. 1969, 427, 428; también *Wehrhan*, TEDH, Slg. 1973, 1254, 1258, 1273). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40.

⁴⁴³Cfr. *Bleckmann*, DÖV 1993, 840 s.; *el mismo*, NVwZ 1993, 826; *Krück*, en: von der Groeben/Thiesing/Ehlermann (editores), EU-/EG-Vertrag (1997), art. 164, nm. 25, 28; *Pernice*, en: Grabitz/Hilf (editores), Recht EU (1999), art. 164, nm. 58, 60. El mismo TEDH ha concebido a partir del caso *Nold* (Slg. 1974, 491) a los derechos fundamentales como parte de los principios generales del derecho, que él "tiene que defender" (cfr. *Hauer*, Slg. 1979, 3727, 3744 s.) Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40.

Así, en el funcionamiento del Estatuto de la Corte Penal Internacional tiene como fundamento los principios generales del derecho, donde logran que las reglas jurídicas nacionales se conviertan en internacionales. *En el debate de derecho penal internacional fue acuñado el concepto de "do-mestic analogy" para aludir al mero traspaso de una regla jurídica nacional al plano del derecho internacional.*⁴⁴⁴ sin embargo esto dentro de los esquemas romano-germánicos no es suficiente para determinar responsabilidad en planos internacionales, y así se ha manifestado la doctrina al respecto. *Es tan evidente que un concepto semejante no es suficiente para fundamentar un principio general del derecho, como que, por otra parte, también lo es que una investigación de los "major legal systems of the world",*⁴⁴⁵ esto es, en especial del commonlaw y del "civil law", ofrece una suficiente base de derecho comparado.⁴⁴⁶ AMBOS, K. (2006:40). Así mismo debemos tener presente la situación política y jurídica de Estados que no pertenecen al mundo occidental, como es el caso de los estados Islámicos, donde encontramos la posición de Kai Ambos en el siguiente sentido: *Por lo demás, la falta de consideración de sistemas jurídicos no occidentales, en especial del derecho islámico*⁴⁴⁷ —prescindiendo de la carencia de conocimientos idiomáticos del

⁴⁴⁴ *Prosecutor v. Blaskic*, Judgement on the Request of the Republic of Croatia for Review of the Decisión of Trial Chamber II of 18 July 1997, 29.10.1997 (IT-95-14-AR 10%bis), para. 40. Cfr. también *Simma/Paulus*, en: Ascensio/Dcaux/Pellet, Droit international penal (2000), p. 63 s. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40

⁴⁴⁵ *Prosecutor v. Tadic*, Judgement 15.7.1999 (IT-94-1-A), para. 225 (en relación con la comisión en coautoría con base un "common purpose" o "common design"; sobre esto, con más detalles, p. 276 ss. vers. al.). Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40

⁴⁴⁶ Cfr. *Prosecutor v. Kupreskic et al.*, *supra*, nota 25, para. 669: "[...] the Trial Chamber will rely on general principles of international criminal law and, if no such principle is found, on the principles common to the various legal systems of the world, in particular those shared by most civil law and common law criminal systems" (resaltado por el autor). Cfr. también *McAuliffe de Guzman*, en: Triffterer (ed.), Commentary (1999), art. 21 nm. 18. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40

⁴⁴⁷ Sobre los ámbitos o familias jurídicas tradicionales en el sentido del derecho comparado cfr. *Zweigert/Kötz*, Rechtsvergleichung (1996), p. 62 ss.; crít. y para una clasificación jerárquica de los ámbitos jurídicos *Heiss*, ZVglRWiss 100 (2001), 396 ss.; crít. también *Husa*,

autor—, puede explicarse, si no justificarse, con que en este trabajo, especialmente en su tercera parte, la comparación jurídica sirve en primer orden a desarrollar dogmáticamente las directrices del ECPI. Por tanto, los “principios generales del derecho en sentido tradicional obtenidos a este respecto cobran importancia, por un lado, para la interpretación del tratado y, por el otro, para colmar lagunas de regulación existentes.”⁴⁴⁸ En este sentido, una limitación al “derecho occidental” es sostenible, pues la versión del ECPI se funda en lo esencial, si no exclusivamente, en la influencia de los Estados del círculo cultural occidental.⁴⁴⁹ AMBOS, K. (2006:41).

4.2. Las competencias del Estado. La dimensión personal de la soberanía

4.2.1. Sobre el reparto de competencias entre los Estados

Uno de los grandes retos del derecho penal internacional es lograr la investigación, juzgamiento y sanción de las conductas macrocriminales que sobrepasan los límites territoriales de los Estados, sin embargo determinar que se han sobrepasado dichos límites y quitar de la esfera de cada Estado la persecución de las conductas delictuales comúnmente genera conflicto entre las naciones involucradas en la comisión de dicha conducta, teniendo a sus asociados como sujetos activos o pasivos de la misma.

R.I.D.C. 2004, 11 ss.Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 40

⁴⁴⁸Sobre ambos puntos de vista desde una perspectiva procesal de derecho penal internacional de la mano del problema de los testigos anónimos en el proceso Tadic, *Affolder*, MichJIL 1998, 486 ss., 492 ss.; sobre el rol del derecho penal comparado en la interpretación del derecho propio, también *Eser*, FS Kaiser (1998), p. 1509 s. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 41

⁴⁴⁹Con ello no se quiere decir que también los Estados no occidentales no hubieran sostenido con empeño sus puntos de vista durante las negociaciones. Citado en: AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis. P. 41

Debemos empezar estableciendo que abarca el concepto de soberanía. En este sentido se han manifestado BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS, así:

La soberanía abarca el conjunto de competencias regladas y discrecionales que el DI atribuye al Estado y que son ejercitables en un plano de independencia e igualdad respecto de los otros Estados. Tal ejercicio bascula, por ello, entre los polos de la soberanía propia y de la soberanía ajena. La coexistencia de una pluralidad de entes soberanos, de Estados, en la sociedad internacional llama, en evitación de conflictos, a la necesidad de articular normas que regulen la distribución de competencias entre ellos. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:817).

Bajo la definición anterior vemos como, en búsqueda de evitar los conflictos por mantener la soberanía, dentro del ámbito del derecho penal internacional, las competencias deben ser repartidas entre los Estados miembros de los tratados que permiten la creación de tribunales internacionales para la aplicación de esta rama del derecho. Y según los autores en cita esta distribución de competencias hace parte de las funciones del Derecho Internacional:

Es ésta una función del DI que ha venido dictada históricamente por la peculiar conformación de estas entidades políticas. La distribución competencial se realiza en concordancia con los elementos característicos del Estado (territorio, población y gobierno). Como entes territoriales que son, su competencia es, en primer lugar, territorial. En

la medida en que cuentan con una población, determinada por el vínculo de la nacionalidad, ejercen una competencia personal sobre los nacionales cuando se encuentran fuera de su territorio. Por último, su condición soberana dota a los Estados de una dimensión exterior, de relación con los otros sujetos internacionales. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:819)⁴⁵⁰.

4.1.1. Sobre la competencia personal del Estado

La competencia o soberanía personal de cada Estado recae sobre los mismos elementos constitutivos de la nación, es decir, personas y territorio, razón por la cual, la soberanía del Estado (sobre su territorio y los asociados que en él se encuentran) tiene el carácter de principal, dejando como subsidiaria la competencia y soberanía de los tribunales internacionales de justicia.

Los autores citados anteriormente definen este fenómeno, así:

“El vigor de la competencia territorial explica el carácter parcialmente subsidiario de la otra base competencial tradicional del Estado: la competencia personal, que se afirma en función de la población, otro de los elementos constitutivos de la condición estatal.

El título válido para la actuación estatal se justifica por tanto en referencia a las personas que, definidas por el vínculo de la nacionalidad, componen su población, y también a los extranjeros

⁴⁵⁰ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

(nacionales de otros Estados o apátridas) que se encuentran sobre el territorio nacional. En este sentido podemos hablar de una dimensión personal de la soberanía territorial. La competencia personal en sentido estricto se proyecta al exterior, siguiendo a los nacionales que se sitúan en territorios no sometidos a la soberanía del Estado de la nacionalidad.

Debe el Estado determinar quienes son sus nacionales, en una operación que guarda ciertas analogías con la determinación de su territorio. Y, una vez establecidos los contornos de esa masa poblacional, a ella —y sólo en el territorio— se le suman las otras personas —extranjeros— que constituyen el todo de la población sobre la que el Estado territorial despliega sus competencias soberanas, con las limitaciones impuestas por el DI. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:820)⁴⁵¹.”

Tenemos entonces a modo de conclusión que la competencia territorial se sobrepone a la competencia personal, pues cada Estado es soberano de ejercer las atribuciones comprendidas en su *Ius Puniendi* a quienes se encuentren en su territorio, por las conductas cometidas en él mismo.

Posteriormente encontramos la teoría de la soberanía personal, donde el Estado persigue para el ejercicio del *Ius Puniendi* a sus asociados, o a quienes cometieron conductas consideradas delictuales en parate de su territorio.

“En puridad, la competencia ejercida sobre nacionales y extranjeros que se encuentra en el territorio del Estado es esencialmente territorial. Por eso decimos que la competencia personal es parcialmente

⁴⁵¹ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). *Derecho Internacional*. Valencia: Tirant Lo Blanch.

subsidiaria de la territorial, porque su invocación resulta superflua cuando se ejerce en el territorio del propio Estado, a menos que se pretenda condicionar el ejercicio de ésta alegando límites vinculados a la extranjería de los interesados.

La concepción cosificada del individuo se ha ido resquebrajando paulatinamente, gracias a la progresión de la normativa internacional sobre los derechos humanos (v. Cap. XXIX), aunque ésta, como comprobaremos, no ha avanzado al punto de afirmar como derechos subjetivos el disfrute efectivo de una nacionalidad o el libre acceso al territorio de un Estado extranjero. La progresión de los derechos de los individuos en cuestiones de nacionalidad y extranjería se ha evidenciado a escala interna, en los ordenamientos de los distintos Estados, sin que por ello pueda afirmarse la emergencia de normas consuetudinarias internacionales. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:821)⁴⁵².

De esa forma se evidencia que los conceptos de competencia, soberanía, derecho penal y derecho penal internacional nunca pueden sobrepasar los límites de los derechos humanos y como lo establecieron los autores citados, la disminución de la cosificación del ser humano gracias al principio de Dignidad Humana es la que permite crear nuevas teorías como la de persecución global de los cibercriminales como se ha realizado en este trabajo investigativo.

4.2. La Responsabilidad Internacional

⁴⁵² BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

4.2.1. Las normas reguladoras de la responsabilidad internacional

Es claro entonces que lo que busca el derecho penal internacional es lograr realizar juicios de reproche y establecer sanciones a los sujetos cuyas conductas delictivas sobrepasen los límites de soberanía territorial de los Estados miembros de cada tratado. Es por eso que deben establecerse normas a seguir en la búsqueda de cada objetivo, por esta razón BROTONS, A.R., Díez-Hochleitner, J., Orihuela Calatayud, E., Pérez-Prat Durbán, L., Riquelme Cortado, R. han establecido:

“Junto a las normas primarias, que establecen las conductas exigibles a los sujetos internacionales, es preciso que existan normas secundarias, para determinar qué sucede cuando se incumplen las normas primarias. El régimen de la responsabilidad abarca el conjunto de reglas que regulan las consecuencias de conductas lesivas a lo prescrito.

La variedad de situaciones en que un sujeto puede comprometer su responsabilidad internacional es tan amplia como el conjunto de obligaciones que haya asumido, de normas primarias con las que se haya comprometido. La fuerza expansiva que viene demostrando en las últimas décadas el DI complica más el cumplimiento por los Estados de obligaciones asumidas sin una comprensión adecuada de su alcance o sin una preparación técnica suficiente. Y, aún así, deben los Estados hacer frente a todas ellas pues, en caso contrario, su infracción genera responsabilidad internacional.

Las normas generales sobre la responsabilidad internacional tienen una acusada impronta de origen consuetudinario, aunque abundan cada vez más los regímenes convencionales que, al regular aspectos concretos de las relaciones internacionales, avanzan también soluciones específicas al eventual incumplimiento por los Estados partes. Lo incierto, lo proteico, lo evolutivo, de este sector del ordenamiento internacional explica que haya constituido un tema central en la agenda de la CDI desde el comienzo de sus tareas, en 1949, consumiendo las energías de más de media docena de relatores especiales antes de la aprobación definitiva en 2001 de un proyecto de artículos sobre responsabilidad internacional de los Estados por hechos internacionalmente ilícitos del que la AGNU tomó nota (res. 56/83, de 28 de enero de 2002). (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:821)⁴⁵³.”

Es en nuestro criterio la amplia variedad de legislaciones lo que ha llevado a los Estados a determinar que las normas que regulas el Derecho Penal Internacional provengan del derecho consuetudinario y no de un modelo taxativo como el romano-germánico que desde el ámbito de la tipicidad no permitiría la persecución penal de las conductas que taxativamente no estén relacionadas en su normatividad.

4.3. Invocación de la responsabilidad y Aplicación coactiva del Derecho Internacional

⁴⁵³ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

Hemos definido anteriormente que el objetivo del Derecho Penal Internacional es la persecución de conductas macrocriminales. Para el caso que nos ocupa vemos al Derecho Penal Internacional como la herramienta para generar sanciones y cumplimiento de ellas de forma efectiva para los autores de ciberdelitos.

Frente a la aplicación coactiva y sancionatoria efectiva del Derecho penal internacional tenemos el claro ejemplo planteado por los autores en cita, así:

Satisfacer la responsabilidad internacional por la comisión de un acto ilícito es una obligación que incumbe a cualquier sujeto, Estado u OI, que haya infringido una obligación internacional. Al igual que sucede con la observancia espontánea del Derecho, puede ocurrir que un infractor haga frente voluntaria, adecuada y rápidamente a su responsabilidad, asumiendo las consecuencias (cesación, reparación, garantías de no repetición), pero la natural resistencia de los sujetos a aceptar que han violado el DI lo hace improbable. Determinar, pues, la comisión —y atribución del ilícito— es una cuestión previa cuya respuesta, necesaria, ha de facilitar el camino para hacer efectiva —si procede— la responsabilidad internacional.

*En el marco de Organizaciones y regímenes internacionales es frecuente contar con mecanismos colegiados que proveen a estas tareas. Son la *lexspecialis* que deja a salvo el Proyecto de arts. sobre responsabilidad del Estado por hechos internacionalmente ilícitos (CDI, 2001, art. 55).*

Así, la Comisión Europea tiene poder para dictaminar que un Estado ha infringido las obligaciones que le incumben en virtud del TCE. Realizada tal constatación, si el Estado no se aquieta podrá demandarlo ante el TJ (TCE, art. 226). También los Estados miembros

pueden demandar, bajo determinadas condiciones, a aquel que en su opinión está incumpliendo el Tratado (TCE, art. 227), El Estado declarado infractor por el TJ ha de tomar las medidas necesarias para ejecutar la sentencia y si no lo hace se expone a ser condenado al pago de una suma a tanto alzado y a multas coercitivas (TCE, art. 228). (BROTÓNS, A.R., Díez-Hochleitner, J., Orihuela Calatayud, E., Pérez-Prat Durbán, L., Riquelme Cortado, R. 2007:821)⁴⁵⁴.”

Nos encontramos ahora frente a la situación de falta de legislación al respecto de una conducta que ha atentado efectivamente bienes jurídicos tutelados por diferentes Estados, lo que genera claramente que si la conducta no esta constituida como delito no tendrá una sanción específica y materializar el juicio de reproche que logre realizarse será imposible.

No obstante lo anterior, los autores en cita han planteado la solución a esta situación, así:

“Pero si no existen normas especiales sobre la existencia del ilícito, el contenido de la responsabilidad o el modo de hacerla efectiva, serán pertinentes las normas del DI general cuya exigencia corresponde al Estado o Estados lesionados (Proyecto de 2001, art. 42) y sólo en determinados casos, atendiendo a la naturaleza de la obligación violada, a otros Estados, no lesionados (art. 48). En su comentario la CDI aclara que la invocación de la responsabilidad se refiere a la facultad de adoptar medidas legales contra el Estado infractor, bien sea la presentación de una reclamación internacional, bien la de una demanda ante un tribunal internacional.

⁴⁵⁴ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

No debe confundirse la invocación de la responsabilidad con el ejercicio, mediante la protesta, de la crítica política. Así cabe interpretar, por ej., la nota de 29 de abril de 2005 dirigida por la Cancillería de la República Argentina a cada uno de los Estados miembros de la U E por la consideración de las Islas Malvinas como territorio de ultramar en el Tratado por el que se establece una Constitución para Europa (Anexo II). Es obvio que un interés jurídico respalda la nota diplomática que no parece destinada, sin embargo, a exigir una responsabilidad internacional a título de Estado lesionado. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:792)."

4.4. Aplicación coactiva del Derecho Internacional

Como se planteó anteriormente, uno de los grandes retos del Derecho internacional y más aun del Derecho Penal Internacional es demostrar que puede ser coactivo, de modo que los Estados no teman asumir los retos de entregar competencia a un tribunal internacional como se pretende para el caso de persecución de ciberdelincuentes.

Frente a las dificultades de aplicación coactiva del Derecho Internacional, los autores previamente citados se han manifestado así:

"Se ha sostenido con insistencia y reiteración que el DI carece de un sistema de aplicación coactiva, afirmación de la que se deduce: 1) la limitadísima eficacia de las normas internacionales, que quedarían al albur de su observancia espontánea; y 2) la negación misma de la juridicidad del DI. Este planteamiento, ya considerado, parte de una errónea apreciación, tanto del fenómeno jurídico como del significado

de la coacción. Ni el Derecho es siempre sinónimo de coacción reglamentada, ni carece el DI de un sistema de aplicación coactiva de sus normas y obligaciones, gracias en parte a: 1) un proceso —ciertamente desigual— de internalización que le permite beneficiarse de los sistemas estatales de ejecución forzosa; y, 2) un proceso de institucionalización —incompleta, pero progresiva— de la sociedad internacional, que ha supuesto aportaciones del orden que ahora comentamos.” (BROTÓNS, A.R., DíEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:795)⁴⁵⁵.”

En palabras de BROTÓNS, A.R., DíEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R., es cierto que el DI, que carece de una jurisdicción obligatoria para el arreglo de las controversias, tampoco cuenta con una OI universal competente para reaccionar mediante el ejercicio de la coacción ante la comisión de ilícitos internacionales. La función que desempeña el C. de S. de las NU no es tal, aunque pudiera pensarse lo contrario, porque si bien la competencia que ejerce en el ámbito del mantenimiento de la paz y de la seguridad internacionales —Capítulo VII de la Carta— le permite adoptar medidas (vulgo, *sanciones*) contra Estados que desde luego han cometido ilícitos internacionales, su actuación se encuentra doblemente limitada, al operar sólo ante una situación de amenaza o quebrantamiento de la paz y la seguridad internacionales o un acto de agresión (art. 39 de la Carta de la ONU) —lo que deja al margen de su actividad la mayoría de ilícitos internacionales— y ser el ejercicio de su competencia de naturaleza política y no jurisdiccional, lo que comporta la sujeción de su intervención en la práctica a criterios de mera oportunidad. (BROTÓNS, A.R., DíEZ-HOCHLEITNER, J., ORIHUELA

⁴⁵⁵ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:821)⁴⁵⁶.” Sin embargo es precisamente esta situación la que buscamos solucionar como desarrollo investigativo en la presente tesis doctoral, nuestro objetivo es la determinación de organismos y procedimientos con la competencia y jurisdicción suficientes para que el Derecho Penal internacional no sea considerado precario dentro de su carácter coactivo, cualidad que no puede faltar dentro de ninguna rama del derecho, toda vez que desvirtua la razón de ser de esta ciencia. Como medida provisional han considerado los autores en cita que si existe algún tipo de solución al conflicto de la característica de coactivo:

“Pero sí existe un conjunto de normas generales de carácter consuetudinario sobre la aplicación coactiva del DI, la mayoría de las cuales tiene que ver con una aplicación descentralizada, que opera tradicionalmente, pero no sólo, en el ámbito de las relaciones bilaterales, así como reglas en numerosos tratados internacionales constitutivos de regímenes y OI. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:795)⁴⁵⁷”

4.5. Protección internacional de los Derechos Humanos

4.5.1. Consideraciones generales

Tal y como se estableció previamente en la investigación, dentro del establecimiento de un proceso, procedimiento y órganos competentes para la

⁴⁵⁶ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

⁴⁵⁷ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

investigación, juzgamiento y sanción de ciberdelitos dentro del plano internacional debe garantizarse como primera medida y bajo los parámetros de los principios universales del derecho y del derecho penal, el respeto y garantía se los derechos humanos, considerados como universales, para lograr así mismo, la aplicación de una justicia universal también.

En este sentido se manifestaron BROTONS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R., diciendo que *todos los derechos humanos son universales, indivisibles e interdependientes y están relacionados entre sí*", dispuso la *Declaración y Programa de Acción de Viena adoptada por consenso de los más de ciento setenta Estados reunidos en la Conferencia Mundial de Derechos Humanos (1993) y ha sido reiterado por todos los miembros de las NU al instaurar, el 15 de marzo de 2006, el Consejo de Derechos Humanos (AG, res. 60/251). Universalidad, indivisibilidad e interdependencia, he ahí los pilares conceptuales en que trata de sustentarse el reconocimiento y protección internacional de los derechos humanos. (BROTONS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:1181)*⁴⁵⁸

4.5.2. Universalidad e Imperatividad

Frente a los principios de universalidad e imperatividad de los derechos humanos y que pretendemos hacer valer para la aplicación de la justicia penal internacional en los casos de ciberdelitos, es necesario conocer sus características en los ámbitos internacionales y en relación a la soberanía de los Estados.

⁴⁵⁸ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

En este aspecto se han manifestado *BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R.* cuando aseguran que *La universalidad es inherente a los derechos humanos fundamentales porque se trata de derechos que son expresión de la dignidad intrínseca de todo individuo, debiendo, en este sentido, ser aceptados y respetados por todos los Estados, con independencia de su sistema ideológico-político, económico y socio-cultural. La Carta de las NU lo expresa de forma categórica exigiendo en su preámbulo su cumplimiento como esencial condición de paz y comprometiéndose (art. 55) a promover su respeto universal. Esta concepción, asumida por la no en balde titulada Declaración Universal de Derechos Humanos (1948) y los numerosos instrumentos que la han desarrollado, fue confirmada por la Conferencia Mundial que, si bien llama la atención sobre la "importancia de las particularidades nacionales y regionales, así como de los diversos patrimonios históricos, culturales y religiosos", salvaguarda al fin el carácter universal de los derechos y libertades, sobre el que "no admite dudas" (Declaración y Programa de Acción de Viena, Parte I, párs. 1 y 5). (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:1183)⁴⁵⁹.*"

Frente al tema de las particularidades culturales que encontramos en la diversidad de Estados que pueden hacerse miembros de cada organización para la persecución de delitos en el ámbito del derecho penal internacional es necesario acatar las recomendaciones de los autores citados en cuanto al relativismo de algunos sistemas políticos. Así:

Debemos, pues, acercarnos con cautela al relativismo que predicán ciertos Estados (principalmente del mundo islámico, pero no sólo de él)

⁴⁵⁹ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

en tanto puede ser la coartada para la violación de derechos fundamentales de individuos bajo su jurisdicción. No obstante, conviene hacer dos precisiones:

1) Si las diferencias culturales y religiosas, y aun las desigualdades económicas que persisten y se alargan como crueles realidades de la sociedad internacional actual, no deben alzarse como barrera contra el carácter universal de los derechos humanos fundamentales, tampoco la normalización de los valores subyacentes ha de convertirse en un instrumento de la dominación de los Estados del Primer Mundo sobre el resto. Una cosa es articular una política global de derechos humanos y otra, menos respetable, es politizarla, es decir, poner esa política al servicio de otras mediante comportamientos selectivos. Los países más poderosos no saben hurtarse a la tentación de hacer política —no de— sino con los derechos humanos.

2) La universalidad de los derechos humanos fundamentales no es incompatible, sino todo lo contrario, con la cooperación regional para su salvaguardia. Es obvio que la mayor afinidad de los vecinos de una región culturalmente homogénea facilita un enunciado más amplio y preciso de derechos y, en particular, una articulación orgánica y procesal más profunda y eficaz de control y garantía (v. infra).

Si la universalidad no ha de ser una expresión retórica, ha de concentrar su acción en el núcleo irreductible de derechos que componen esferas de protección prioritaria: represión de los actos de genocidio, crímenes de guerra y contra la humanidad, abolición de la

esclavitud y la discriminación racial, lucha contra la tortura y otros tratos crueles, inhumanos y degradantes, abolición de la pena de muerte (al menos, por delitos cometidos por personas menores de edad); asimismo, ha de identificar los grupos humanos más vulnerables a la violación de sus derechos y libertades fundamentales: pueblos indígenas, refugiados, apátridas, emigrantes, mujeres, niños, reclusos, discapacitados..., haciéndolos beneficiarios de una protección particular. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:1182)⁴⁶⁰.”

Como lo han planteado los autores citados frente a la universalidad como objetivo presente en la Carta de las NU y en la *Declaración Universal* adquiere verdadera significación respecto de los derechos y libertades fundamentales que han dado vida a obligaciones *erga omnes* nacidas, en su núcleo duro al menos, de normas *imperativas* de DI. Se trata de los derechos a la vida y sus corolarios más inmediatos (garantías contra la esclavitud, la tortura, las detenciones y penas arbitrarias...), que no admiten suspensión bajo ninguna circunstancia o condición (Pactos de NU, 1966, art. 4; Convenio Europeo, art. 15; Convención Americana, art. 27). Podría así decirse que la *universalidad* de los derechos humanos fundamentales y su *imperatividad* internacional forman un tándem indisociable. Podemos a través de la analogía determinar que lo que buscamos proteger bajo la teoría y presupuestos del derecho penal internacional, que para este caso concreto son los derechos de protección a la información y a los datos, que se vulneran a través de la comisión de CIBERDELITOS, puede considerarse en esta época de globalización como derecho fundamental e inherente al ser humano, ya que de la utilización de

⁴⁶⁰ BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.

cada tipo de información y datos se desprenden asuntos de tanta trascendencia como la seguridad, el patrimonio económico, la honra, el honor, las libertades e integridad sexuales, y un sin número de bienes jurídicos tutelados comúnmente en la mayoría de Estados occidentales.

A modo de ejemplo los autores en cita han planteado:

Es justamente este el sentido en el que hace cerca de cuarenta años la CU admitió (Barcelona Traction, 1970), que "la prohibición de los actos de agresión, del genocidio y los principios y reglas relativos a los derechos fundamentales de la persona humana" son normas de iuscogensen la medida que representan "obligaciones de los Estados hacia la comunidad internacional en su conjunto". Años después la Corte ha tenido la ocasión de confirmar el carácter erga omnes de los derechos y obligaciones consagrados por la Convención para la prevención y sanción del delito de genocidio (Aplicación de la Convención para la prevención y represión del crimen de genocidio (Bosnia y Herzegovina c. Serbia y Montenegro, 1996) y de algunas disposiciones de los Pactos de NU (1966) y del Cuarto Convenio de Ginebra (1949) (Consecuencias jurídicas derivadas de la construcción de un muro en el territorio palestino ocupado, 2004). Se le han planteado incluso algunos asuntos.

Que bajo la piel de las obligaciones en materia consular del Estado receptor frente al Estado que envía y a sus nacionales planteaban cuestiones que afectaban un derecho fundamental, como el de la vida frente a la pena de muerte, aunque la Corte haya optado por mantenerse en la tierra firme sobre la que se asentaba su jurisdicción {LaGrand, 2001; Avena y otros subditos mexicanos, 2004}.

Las violaciones de los derechos y libertades en 2006 siguen alcanzando unas proporciones sin precedentes, en un crescendo cuyas cénit escapa a la imaginación. El Informe que Amnistía Internacional publicó en 2006 sobre el estado de los derechos humanos en el mundo durante 2005 constataba violaciones en ciento cincuenta países, afirmaba la manipulación por los gobiernos poderosos de la ONU y las instituciones regionales en beneficio de sus mezquinos intereses nacionales y en detrimento de los derechos humanos, señalando a Estados Unidos como ejemplo destacado de ello, pero no el único, "como ponen de manifiesto —dice el informe— el historial de Rusia en el Cáucaso y en Asia Central y la creciente cooperación económica de China con algunos de los gobiernos más represivos de África". Es así como se sigue verificando el genocidio, la tortura, la intolerancia étnica y religiosa, la violencia contra la mujer y la infancia, las detenciones arbitrarias y desapariciones forzadas, las ejecuciones extrajudiciales o sumarias,..., violaciones facilitadas y agravadas por los conflictos armados, el uso y abuso de la declaración de estado de excepción, así como por la situación de tiranía, extrema pobreza y endeudamiento exterior que padece un gran número de ellos. (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007. P 1181-1183)

4.5.3. Indivisibilidad e Interdependencia

Dentro de los principios y fundamentos de interpretación y aplicación de los derechos humanos, que deben regir la aplicación de sistemas de justicia internacional, como el que buscamos establecer con la presente tesis, encontramos los presupuestos de Indivisibilidad e interdependencia, definido

por BROTONS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. cuando dice *Que todos los derechos y libertades fundamentales constituyen en esencia una unidad es el segundo gran principio que ha de inspirar su promoción y respeto.* Esto teniendo como antecedente que el primer principio de interpretación de derechos humanos es el de universalidad que fue analizado en el numeral anterior.

Según los dos principios estudiados en este aparte de la investigación, todas las categorías de los derechos humano, en palabras del autor en cita *Derechos civiles y políticos, económicos, sociales y culturales y los más controvertidos derechos de solidaridad —derechos humanos de primera, segunda y tercera generación, según se dice— están unidos por vínculos indisolubles que dan forma a un conjunto indivisible e interdependiente.* Quiere decir lo anterior que es de obligatorio cumplimiento para todos los Estados firmantes de la convención de Viena darle estas características y aplicar estos principios en la ejecución de sus acciones públicas dirigidas a los asociados, y la aplicación de los principios no puede tener relación directa con el grado de desarrollo de cada Estado, es por esta razón que el autor en cita establece que *no es por eso de recibo enarbolar el subdesarrollo para justificar atentados a los derechos civiles y políticos (libertad, igualdad, seguridad, participación en la vida pública...), alegando que así se propicia más eficazmente el desarrollo económico y social de la población. El subdesarrollo condiciona, merma, desde luego el disfrute de los derechos humanos, pero no debe ser invocado como excusa absolutoria de su vulneración más flagrante (Declaración de Viena, 1993, Parte I, par. 10).* BROTONS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. (2007:1184).

Otra de las características que compone este principio radica en que *la indivisibilidad e interdependencia de todos los derechos humanos impone también denunciar la discriminación en las obligaciones asumidas por los Estados y los mecanismos institucionales y procesales dispuestos para su observancia, que ha favorecido a los derechos civiles y políticos, a los que la misma Declaración Universal dedicó diecinueve de sus treinta artículos.* BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. (2007:1184).

Dentro de las obligaciones de los Estados frente al cumplimiento de los derechos civiles y políticos y los derechos económicos sociales y culturales encontramos que los primeros generan una responsabilidad de resultado mientras que los segundos generan responsabilidades de medios, así lo explican los autores citados en párrafos anteriores:

“A diferencia de los derechos civiles y políticos, que imponen a los Estados obligaciones de resultado, los económicos, sociales y culturales se traducen en obligaciones de comportamiento progresivo, supeditadas a la disponibilidad de recursos y a la política económica y social estatal. Hay una relativización de la obligación de asegurar el ejercicio de estos derechos que inevitablemente se proyecta en los límites impuestos a su justiciabilidad en los ordenamientos internos y, asimismo, condiciona los mecanismos, más blandos, establecidos para controlar su cumplimiento a nivel internacional. BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. (2007:1185).”

Es de esta forma que encontramos la relación directa de la aplicación de estos principios con la búsqueda de la paz y justicia internacional que es precisamente nuestro objetivo investigativo con esta tesis, que se pueda ejercer el derecho a la justicia de forma universal para los casos de ciberdelitos, de modo que los límites territoriales no sean un impedimento para ello. En este sentido se ha pronunciado los autores citados cuando dicen:

“No obstante, la reivindicación de los derechos colectivos ha coadyuvado a generalizar la conciencia de que cualquier estrategia en pro del respeto de los derechos humanos sólo será posible mediante la acción concertada de todos los actores de la escena interna e internacional (particularmente Estados y OI). Por otro lado, la solidaridad, el objetivo de paz positiva, que subyace en los nuevos derechos es una garantía, un aval, para el cumplimiento de los derechos tradicionales, de la misma forma que el disfrute de éstos ha de beneficiar a aquéllos.

Así pretende significarlo el informe de 2005 (21 de marzo) del Secretario General, Kofi Annan, en el mismo título, Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos, para a continuación subrayar que "el desarrollo, la seguridad y los derechos humanos no sólo son indispensables sino que se refuerzan mutuamente. [...] Así pues, no tendremos desarrollo sin seguridad, no tendremos seguridad sin desarrollo y no tendremos ninguna de las dos cosas si no se respetan los derechos humanos" (párs. 16 y 17). (BROTÓNS, A.R., DÍEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PEREZ-PRAT DURBÁN, L., RIQUELME CORTADO, R. 2007:1185)”

4.6. La Corte Penal Internacional como asociación voluntaria de Estados.

En estadios anteriores de la presente investigación nos encargamos de empezar a definir los principios, fundamentos y características de los derechos humanos universales e inherentes al ser humano, cuya protección y mantenimiento es obligación inviolables de los Estados que voluntariamente han sido parte de los tratados y convenciones.

Lo anterior en búsqueda de una solución que permita la investigación, juzgamiento y sanción de las conductas delictivas que atenten contra y a través de la información y los datos a los asociados y/o a los Estados, y que las hemos denominado con ayuda de la doctrina jurídica como Ciberdelitos, de forma universal. Hemos establecido que esta persecución penal debe realizarse en sujeción al principio de universalidad debido a que estas conductas sobrepasan los límites de jurisdicción y competencia territorial de los Estados, y en esta lucha por aplicación de cada una Puniendi Estatal se pierde el objetivo de generar justicia universal y muchos delitos no logran ser juzgados ni sancionados.

Es por las anteriores razones que en este momento investigativo plantearemos por primera vez y a modo introductorio que el órgano internacional que debe mantener la jurisdicción y competencia para la investigación, juzgamiento y sanción de los ciberdelitos debe ser la Corte Penal Internacional como Organización Internacional, razón por la que hemos acudido a diferentes autores para empezar a desarrollar este presupuesto.

Entendiendo a la Corte Penal Internacional como Organización Internacional empezamos su caracterización con las definiciones establecidas por

BLÁSQUEZ PEINADO⁴⁶¹, quien establece que *el primer rasgo que caracteriza a las Organizaciones Internacionales es el de haber sido constituidas por Estados, sin perjuicio de que en algunas de ellas puedan participar, incluso como miembros de pleno derecho, otras Organizaciones Internacionales (así, por ejemplo la Comunidad Europea en la FAO, la ONU o la OMC). Los Estados, sujetos primigenios del Derecho internacional, son los que crean voluntariamente las Organizaciones internacionales —sujetos derivados o secundarios del Derecho Internacional— convirtiéndose de este modo en miembros de las mismas.* BLÁSQUEZ PEINADO, M.D. (2003:111).

Vemos entonces en la definición anterior que la CPI se ha constituido por Estados, quienes tienen la capacidad de hacerse parte y definir los límites de su propia soberanía y jurisdicción, en este caso concreto para la persecución de ciberdelitos. Para Blásquez Peinado, *La Corte Penal Internacional también debe su existencia a la voluntad de los Estados. Son los Estados de la Sociedad Internacional, o al menos una buena parte de ellos, los que han llevado a cabo las negociaciones para el establecimiento de la Corte, los que han firmado el Estatuto de Roma y los que han manifestado su consentimiento en obligarse por dicho instrumento jurídico internacional. Los Estados son en definitiva, como sucede en todas las Organizaciones internacionales, los miembros de la Corte Penal Internacional, aunque el Estatuto no se refiera a ellos con esta denominación y prefiera la de Estados partes. Ahora bien, a pesar de ser esto así, existen algunas especialidades que diferencian a la Corte de las Organizaciones internacionales tradicionales y que se refieren a los requisitos exigidos para ser parte de la organización, a los modos de adquisición y pérdida de la condición de Estado parte y al papel que otros*

⁴⁶¹ BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach

sujetos distintos de los Estados jugaron en su creación. El Estatuto de Roma no prevé, a diferencia de lo que sucede en los Tratados constitutivos de otras Organizaciones internacionales⁴⁶², unos requisitos sustantivos o de fondo que los Estados miembros deban reunir para poder formar parte de la Corte. El único requisito exigido, de carácter formal, es la prestación del consentimiento a través de cualquiera de los procedimientos previstos a tal efecto por el Estatuto. Tampoco existe a este respecto distinción alguna entre Estados miembros originarios y sobrevenidos a diferencia de lo que sucede en el resto de las Organizaciones internacionales. En ellas, por norma general, la aceptación de miembros sobrevenidos se supedita a un procedimiento en el que pueden participar las instituciones u órganos de la Organización y en el que los Estados partes, pueden vetar la incorporación de los nuevos miembros⁴⁶³. BLÁSQUEZ PEINADO, M.D. (2003:113)

⁴⁶²En este sentido, el artículo 4.1. de la Carta de San Francisco establece que: «Podrán ser Miembros de las Naciones Unidas todos los demás amantes de la paz que acepten las obligaciones consignadas en esta Carta, y que, a juicio de la Organización, estén capacitados para cumplir dichas obligaciones y se hallen dispuestos a hacerlo. Por su parte el artículo 49 del TUE establece como requisitos de fondo para la adhesión a la Unión europea, el ser un Estado europeo que respete los principios de libertad, democracia, respeto de los derechos humanos y las libertades fundamentales. Además, y aunque el Tratado no lo prevé expresamente, otros requisitos imprescindibles para adherirse a la Unión europea son el de tener una economía de mercado mínimamente eficaz y la aceptación íntegra del acervo comunitario por parte de los nuevos Estados. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.113

⁴⁶³Vid. a modo de ejemplo, el artículo 10 del Tratado de Washington, constitutivo de la OTAN, que prevé un derecho de veto por parte de los Estados miembros en relación con la entrada de nuevos miembros, al exigir que ésta debe de hacerse por acuerdo unánime de los Estados miembros. En el mismo sentido, el artículo 4.2. de la Carta de Naciones Unidas establece que la admisión de nuevos miembros será decidida por la Asamblea General a recomendación del Consejo de Seguridad. Por su parte, el artículo 49 del Tratado de la Unión Europea establece un procedimiento formal de adhesión a la Unión en dos fases. En la primera intervienen las instituciones comunitarias (el Estado adherente debe solicitar su ingreso ante el Consejo, quién deberá pronunciarse por unanimidad después de haber consultado a la Comisión y previo dictamen conforme del Parlamento europeo que se pronuncia por mayoría absoluta de los miembros que lo componen). En la segunda fase intervienen los Estados miembros por un lado, y los adherentes por otro, que deben, todos y cada uno de ellos, firmar y ratificar el acuerdo de adhesión en el que se fijan las condiciones de admisión de los nuevos socios y las adaptaciones que esta admisión suponga, de acuerdo con sus respectivas normas constitucionales. Vid. a modo de ejemplo, el artículo 10 del Tratado de Washington, constitutivo de la OTAN, que prevé un derecho de veto por parte de los Estados miembros en relación con la entrada de nuevos miembros, al exigir que ésta debe de hacerse por acuerdo

Hemos establecido ya diferentes características de la Corte Penal Internacional que a todas luces demuestran ventajas en su funcionamiento y procedimientos que permitirían eventualmente entregarle al competencia principal para persecución y efectos coactivos en materia de Ciberdelitos, uno de sus principales presupuestos que nos permiten colegir que se lograría radica en que *mediante la prestación del consentimiento para obligarse por el Estatuto, el Estado no sólo se incorpora a la Corte, sino que además reconoce automáticamente la competencia de ésta para enjuiciar determinados crímenes internacionales cometidos en su territorio o por sus nacionales. No se requiere por tanto, como sucede en otras Organizaciones internacionales, un acto posterior de aceptación de la jurisdicción de la Corte. En este particular la Corte Penal Internacional se distancia de los tribunales de las Organizaciones internacionales de cooperación (por ejemplo, el Tribunal Internacional de Justicia)*⁴⁶⁴*asemejándose al órgano jurisdiccional de una*

unánime de los Estados miembros. En el mismo sentido, el artículo 4.2. de la Carta de Naciones Unidas establece que la admisión de nuevos miembros será decidida por la Asamblea General a recomendación del Consejo de Seguridad. Por su parte, el artículo 49 del Tratado de la Unión Europea establece un procedimiento formal de adhesión a la Unión en dos fases. En la primera intervienen las instituciones comunitarias (el Estado adherente debe solicitar su ingreso ante el Consejo, quién deberá pronunciarse por unanimidad después de haber consultado a la Comisión y previo dictamen conforme del Parlamento europeo que se pronuncia por mayoría absoluta de los miembros que lo componen). En la segunda fase intervienen los Estados miembros por un lado, y los adherentes por otro, que deben, todos y cada uno de ellos, firmar y ratificar el acuerdo de adhesión en el que se fijan las condiciones de admisión de los nuevos socios y las adaptaciones que esta admisión suponga, de acuerdo con sus respectivas normas constitucionales. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.113

⁴⁶⁴En el ámbito de Naciones Unidas, el hecho de ser parte en la organización y, consecuentemente, en el Estatuto del TU, no conlleva automáticamente la aceptación de la competencia del Tribunal, sino que esa aceptación es un acto voluntario y facultativo Vid. el artículo 36.2 del Estatuto del Tribunal Internacional de Justicia, que se refiere a la jurisdicción obligatoria del TU mediante la aceptación de la llamada «cláusula facultativa». A tenor de la misma: «Los Estados Partes en el presente Estatuto podrán declarar en cualquier momento que reconocen como obligatoria *ipso facto* y sin convenio especial, respecto de cualquier otro Estado que acepte la misma obligación, la jurisdicción de la Corte en todas las controversias de orden jurídico que versen sobre: a) la interpretación de un Tratado, b) cualquier cuestión de derecho internacional, c) la existencia de todo hecho que, si fuera establecido, constituiría violación de una obligación internacional, d) la naturaleza o extensión de la reparación que ha de hacerse

*Organización internacional de integración (el Tribunal de Justicia de las Comunidades Europeas)*⁴⁶⁵. BLÁSQUEZ PEINADO, M.D. (2003:114). Teniendo en cuenta esta característica, entregar a la Corte Penal Internacional la jurisdicción para persecución de ciberdelitos no implicaría modificaciones en la manifestación de voluntad de sus Estados Partes o de los futuros o a unirse, toda vez que es precisamente este procedimiento, o en otras palabras la falta de este, lo que la diferencia de otros tribunales internacionales de justicia.

Frente a la situación de pérdida de la condición de Estado Parte de la Corte Penal Internacional, de conformidad al Estatuto, el autor en cita ha establecido:

“En cuanto a la pérdida de la condición de Estado parte, ésta sólo puede producirse de modo voluntario, por denuncia, ya que el Estatuto no prevé ningún sistema de expulsión, a diferencia de lo que sucede

por el quebrantamiento de una obligación internacional». Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.114

⁴⁶⁵En el ámbito de las Comunidades Europeas, la jurisdicción del Tribunal de Justicia de las Comunidades europeas es aceptada automáticamente por los Estados miembros de la Organización desde el momento de la pertenencia o adhesión a la misma sin que sea necesario un acto de aceptación ulterior por parte de dichos Estados. En este particular, nótese que nos referimos a las Comunidades europeas y no a la Unión Europea, globalmente considerada, porque en ésta, concretamente dentro del pilar de la Cooperación Policial y Judicial en materia penal, y respecto de algunas cuestiones determinadas (cuestiones prejudiciales sobre la interpretación y validez de decisiones y decisiones marco y sobre la interpretación de convenios internacionales), sí es preciso, después del Tratado de Amsterdam, una declaración que deje clara la voluntad de los Estados de aceptar la competencia del TJCE. Vid. en este sentido, el artículo 35 del TUE. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.114

en algunas Organizaciones internacionales⁴⁶⁶. Dicha denuncia surtirá efectos, de conformidad con el Estatuto, un año después de su notificación al Secretario General de las Naciones Unidas, a menos que en ella se indique una fecha ulterior⁴⁶⁷. La denuncia no exime al Estado de las obligaciones que hubiera contraído mientras era parte en el Estatuto, en concreto de las de carácter financiero y tampoco será un obstáculo a que el Estado siga cooperando con la Corte en las investigaciones y enjuiciamientos en relación con los cuales el Estado esté obligado a cooperar y que se hayan iniciado antes de la fecha en que la denuncia surta efecto⁴⁶⁸. Lo que sí prevé el Estatuto es la suspensión de determinados derechos inherentes a la condición de miembro (el derecho de voto en los órganos políticos) en el caso de que el Estado haya incurrido en el impago de sus contribuciones financieras por un importe correspondiente a las cuotas de los dos años

⁴⁶⁶La Carta de Naciones Unidas prevé expresamente, en su artículo 6 la expulsión de cualquier miembro que haya violado repetidamente los principios contenidos en ella. Esta medida, que se decide por la Asamblea General a recomendación del Consejo de Seguridad, no ha sido aplicada hasta la fecha. El Tratado de la Unión europea no prevé, por su parte, la posibilidad de expulsión de un miembro de la Unión. Todo lo más, el artículo 7 del TUE, tal y como fue modificado por el Tratado de Amsterdam, prevé la posibilidad de suspender determinados derechos inherentes a la condición de miembro (en particular el derecho de voto en el Consejo), si se produce una violación grave y sistemática de los principios enunciados en el artículo 6.2 del TUE. Tampoco este procedimiento se ha utilizado hasta el momento en el seno de la Unión Europea. El Tratado de Niza, por su parte, ha añadido un nuevo párrafo a dicho artículo 7 en el que se prevé un mecanismo «de alerta», mediante el que se podrá constatar la existencia de un riesgo claro de violación grave por parte de un Estado miembro de los principios enunciados en el artículo 6.1, pero en cualquier caso, sigue sin preverse la posibilidad de una expulsión de la organización. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.115

⁴⁶⁷Vid. el artículo 127.1 del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.115

⁴⁶⁸Vid. en este sentido, el artículo 127.2 del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.115

*anteriores, a menos que dicho impago se deba a causas ajenas a la voluntad del Estado parte. Esta previsión de suspensión es bastante habitual en los Tratados constitutivos de otras Organizaciones internacionales*⁴⁶⁹.” (BLÁSQUEZ PEINADO, M.D. 2003:115)

Todas la características y especialidades que el autor en cita ha evidenciado sobre la Corte Penal Internacional, así como *la inexistencia en el Estatuto de requisitos de fondo para formar parte de la misma, los escasos requisitos de procedimiento y el hecho de haber sido constituida como un órgano de jurisdicción automática y obligatoria, ponen de manifiesto la voluntad de los Estados de crear una jurisdicción eficaz que al mismo tiempo fuera lo más representativa posible y tuviera el respaldo de la mayoría de Estados de la Sociedad Internacional*. Y esa búsqueda de jurisdicción eficaz y representativa que sea capaz de generar y administrar justicia de forma universal y con sujeción a los principios generales del derecho, a los principios generales del Derecho penal y del derecho penal internacional, y a los derechos humanos con el objetivo de garantizar los derechos colectivos de los asociados de cada Estado son los elementos que nos llevan a concluir que la mejor opción para definir un órgano de justicia internacional para persecución de Ciberdelitos es la Corte Penal Internacional.

A continuación algunas otras características y ventajas de la Corte Penal internacional, planteadas por el autor en cita:

⁴⁶⁹ También la Carta de las Naciones Unidas prevé, en su artículo 5, la posibilidad de suspender a un Estado del ejercicio de los derechos y privilegios inherentes a su calidad de miembro en el caso de que haya sido objeto de acción preventiva o coercitiva por parte del Consejo de Seguridad. Sin embargo tampoco esta medida ha sido aplicada hasta ahora. En relación con el TUE, nos remitimos a lo señalado supra, en anteriores notas a pie de página. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.115

“Los Estados partes en la Corte Penal Internacional ejercen sus derechos en el seno de la Asamblea de los Estados partes. Esta no es en puridad un órgano de la Corte pues formalmente no está integrada en su sistema orgánico⁴⁷⁰, pero juega un papel muy importante tanto en el funcionamiento como en la organización interna de la misma. Se trata de un órgano plenario que presenta importantes similitudes con la Asamblea General de las Naciones Unidas, tanto desde el punto de vista de su composición y funcionamiento, como por las competencias que tiene atribuidas⁴⁷¹. Está compuesta por un representante de cada Estado, acompañados por sus suplentes y asesores. La Asamblea también está abierta a los Estados que simplemente han firmado el Estatuto, y que por tanto no son partes en el mismo, ni miembros de la organización: estos participarán en ella a título de observadores. La Asamblea adopta sus decisiones por consenso y si éste no fuera posible, por mayoría simple o de dos tercios, según que se trate de cuestiones de procedimiento o de fondo⁴⁷².

⁴⁷⁰La Asamblea de Estados partes no se regula en el artículo 34 del Estatuto, dedicado a los órganos de la Corte como tendremos la oportunidad de analizar infra, sino en el artículo 112 del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.116

⁴⁷¹Así, y en claro paralelismo con las funciones ejercidas por la Asamblea General de Naciones Unidas, la Asamblea de Estados partes puede establecer los órganos subsidiarios que considere oportunos (incluido un mecanismo de supervisión independiente que se encargará de la inspección, evaluación e investigación de la Corte), aprobar su propio Reglamento interno, fijar las cuotas o contribuciones de los miembros de la Organización para sufragar los gastos de la misma en el Reglamento financiero de la Corte, examinar y aprobar el presupuesto de la Organización. Además la Asamblea de Estados Partes se reúne, como la Asamblea General de Naciones Unidas, una vez al año, aunque puede celebrar periodos extraordinarios de sesiones cuando las circunstancias lo exijan y podrá utilizar los mismos idiomas de trabajo que la Asamblea General de Naciones Unidas. Vid. el artículo 112, párrafos 4, 5, 9 y 10 del Estatuto, donde se recogen estas funciones. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.116

⁴⁷²Vid. el artículo 112.7 del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales.

Las funciones de la Asamblea serán de dos tipos: unas que ejercerá con carácter permanente y otras que ejercerá con motivo de la puesta en funcionamiento de la Corte⁴⁷³. Entre las primeras, mencionaremos, por su relevancia, las que se refieren a la composición y funcionamiento de la Corte, a cuestiones presupuestarias, al incumplimiento por parte de los Estados de la obligación general de cooperar con la Corte y al arreglo de controversias de tipo no jurisdiccional surgidas entre Estados con ocasión de la interpretación o aplicación del Estatuto⁴⁷⁴. Las segundas son de carácter legislativo y se refieren a la adopción de una serie de instrumentos jurídicos que tienen por objeto el desarrollo del Estatuto y que son imprescindibles para la puesta en funcionamiento definitiva de la Corte, prevista para mediados del año 2003⁴⁷⁵”.(BLÁSQUEZ PEINADO, M.D. 2003:118)

En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.116

⁴⁷³Vid. esta distinción en ESCOBAR HERNÁNDEZ, C. «La Corte Penal Internacional» en *Las Organizaciones.....op. cit.*, págs. 436 y 437. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.117

⁴⁷⁴Vid. en relación con estas funciones, el artículo 112. 2.e) en relación con el artículo 36,112.2.d), 112.2.f) y 119, respectivamente, del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.117

⁴⁷⁵Se trata de las Reglas de Procedimiento y Prueba, de los Elementos de los Crímenes, del Acuerdo con las Naciones Unidas, del Acuerdo de Sede con los Países Bajos, del Acuerdo sobre Privilegios e Inmunidades de la Corte, del Reglamento de la Asamblea, del Reglamento Financiero y del Reglamento de Personal. Estos instrumentos jurídicos son aprobados por la Asamblea de Estados Partes sobre la base de las propuestas sometidas por la Comisión Preparatoria. Dicha Comisión fue establecida en la resolución F del Acta Final de la Conferencia de Roma. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.117

4.6.1. Creación de la Corte Penal Internacional.

Blásquez Peinado en su obra en cita ha mencionado que *una de las cuestiones más discutidas en el seno de la Comisión de Derecho Internacional durante los trabajos para el establecimiento de la Corte fue qué mecanismo debía utilizarse para su creación. No era una cuestión carente de importancia, pues dicho mecanismo condicionaría las ulteriores relaciones de la Corte con las Naciones Unidas*⁴⁷⁶ y, lo que es más importante, *la naturaleza jurídica del nuevo órgano jurisdiccional. Existía un amplio consenso en cuanto a la necesidad de estrechar los lazos entre la Corte y las Naciones Unidas y partiendo de esta base, la Comisión de Derecho Internacional barajó cuatro posibles sistemas de creación de la Corte*⁴⁷⁷: *mediante una resolución de la Asamblea General, mediante una resolución del Consejo de Seguridad, mediante una enmienda de la Carta de las Naciones Unidas y mediante un Tratado internacional. Las cuatro opciones ofrecían ventajas e inconvenientes.* (BLÁSQUEZ PEINADO, M.D. 2003:118).

Finalmente, y luego de amplios debates *La cuarta opción, que se impuso finalmente, suponía la creación de la Corte Penal Internacional por medio de un Tratado internacional. Con ella se evitaba reformar la Carta, las posibles impugnaciones de legitimidad de un órgano creado mediante resolución y se*

⁴⁷⁶Vid. en este sentido, el informe de la CDI sobre la labor realizada en su 46 período de sesiones (A/49/10, par 53). Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.119

⁴⁷⁷Vid. a propósito de esta cuestión, ZAFRA ESPINOSA DE LOS MONTEROS, R. «El establecimiento convencional de la Corte Penal Internacional: grandeza y servidumbres» en AAW *La criminalización de la barbarie: la Corte Penal Internacional*. CGPJ, Madrid, 2000, pág. 159-194. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach P.119

*dejaba total libertad a los Estados para obligarse por dicho Tratado, aceptando en consecuencia la competencia de la Corte*⁴⁷⁸. (BLÁSQUEZ PEINADO, M.D. 2003:118).

Ahora, en palabras del autor previamente citado encontramos la razón fundamental por la cual consideramos que el órgano internacional encargado de la persecución de los ciberdelitos debe ser la Corte Penal Internacional, cuando dice: *“un tratado internacional de las características del Estatuto de Roma nos parece la fórmula más respetuosa con la soberanía estatal teniendo en cuenta que se trata de crear una jurisdicción que, aunque tenga carácter complementario respecto de las jurisdicciones penales nacionales, puede ejercer su competencia si estas últimas no pueden o no quieren actuar, produciéndose, como señalábamos al principio de este trabajo, una importante transferencia del ius puniendi estatal que pasaría a ser ejercitado por un órgano internacional.”* (BLÁSQUEZ PEINADO, M.D. 2003:119). y es precisamente este argumento el que permite adecuar las competencias de la Corte con la voluntad de los Estados para adicionar esta función, pero ya no de forma subsidiaria sino principal.

Quiere decir lo anterior, citando a Blásquez Peinado que *la elección de la vía convencional ha supuesto un cambio importante en relación con la creación de anteriores órganos jurisdiccionales de naturaleza penal internacional. Estos fueron instituidos mediante un acto de autoridad o de naturaleza «legislativa», que no requería el consentimiento de los Estados a los que iban*

⁴⁷⁸Como ha señalado la doctrina, el recurso a la vía convencional tiene la ventaja de garantizar la seguridad en la definición y aceptación de las obligaciones asumidas por los Estados, evita conflictos competenciales que se han suscitado respecto de otras jurisdicciones penales internacionales y favorece el incremento de la legitimación social, elemento esencial para el funcionamiento efectivo de un órgano como la Corte. Vid. en este sentido, Escobar Hernández, C. «La Corte Penal Internacional: rasgos básicos» en AA.W. *Crimen Internacional...op. cit.*, pág. 231. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.120

*dirigidos*⁴⁷⁹. En el caso de la Corte ha habido, por el contrario, un proceso más transparente y abierto a la participación de todos los Estados de la Sociedad Internacional⁴⁸⁰. (BLÁSQUEZ PEINADO, M.D. 2003:120).

La manifestación de la voluntad de los Estados y no la imposición a través de Organizaciones Internacionales de su adhesión al Estatuto de Roma y por consiguiente de sometimiento a las facultades, competencia y jurisdicción de la Corte Penal Internacional genera que no se creen situaciones de conflicto por aplicación del *Ius Puniendi* estatal sobre el universal ejercido, en nuestro caso concreto, por la Corte Penal Internacional, así lo planteado el autor en cita:

“La instauración de la Corte Penal Internacional mediante un tratado internacional permite que los Estados partes definan con claridad las características de la institución que desean crear. En este caso se trata de un órgano independiente⁴⁸¹, no subordinado a ninguna otra institución internacional (sin perjuicio de su vinculación con las

⁴⁷⁹Ello es así con independencia de la naturaleza formal de dicho acto, un acuerdo entre potencias vencedoras en el caso de los Tribunales de Nuremberg y Tokio, o una Resolución del Consejo de Seguridad en los casos de los Tribunales de la ex Yugoslavia y de Ruanda. Vid. a este respecto, YAÑEZ BARNUEVO, J.A. «La Conferencia de Roma y el Estatuto de la Corte Penal Internacional: balance y perspectivas» en AA W. *Creación de una jurisdicción penalop. cit.*, págs. 17-28, pág. 21. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.121.

⁴⁸⁰En este sentido, apunta Yañez que se ha tratado de un proceso abierto y público, típico de las formas de la diplomacia multilateral y más concretamente de los mecanismos utilizados por la Asamblea General de las Naciones Unidas para la codificación y desarrollo progresivo del Derecho Internacional. Vid. YAÑEZ BARNUEVO, J.A. Hacia un Tribunal de la Humanidad: la Corte Penal Internacional. Conferencia de clausura de los Cursos Euromediterráneos Bancaja de Derecho Internacional 2001. Volumen V. En prensa. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.121.

⁴⁸¹Así se establece en el preámbulo del Estatuto de Roma. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.121.

*Naciones Unidas)*⁴⁸², *de carácter permanente*⁴⁸³, *dotado de un sistema institucional propio y estable, de una sede material (situada en La Haya)*⁴⁸⁴ *y con vocación de universalidad, es decir, abierta a la participación de todos los Estados que quieran incorporarse y acepten íntegramente las disposiciones del Estatuto. (BLÁSQUEZ PEINADO, M.D. 2003:122)”*.

Frente a la adhesión y participación del Estado Español en el Estatuto de Roma, tenemos:

*La participación del Parlamento español en la ratificación del Estatuto tuvo la máxima intensidad posible prevista por la Constitución, lo que supone autorización mediante Ley Orgánica*⁴⁸⁵. *Ello pone de relieve la*

⁴⁸²El artículo 2 del Estatuto se refiere a la vinculación de la Corte con las Naciones Unidas por medio de un acuerdo que deberá aprobar la Asamblea de los Estados Partes y concluir luego el Presidente de la Corte en nombre de ésta. Vid. El proyecto de Acuerdo elaborado por la Comisión Preparatoria, en PCNICC/2001/1/Add. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.121.

⁴⁸³ Vid. En este sentido, el artículo 1 del Estatuto que se refiere a la permanencia de la Corte. La permanencia significa que la corte deberá funcionar continuamente, y no reunirse sólo cuando sea necesario para conocer de un asunto determinado, como se señalaba en el proyecto CDI de 1994. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.121.

⁴⁸⁴Vid. el artículo 3 del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.122.

⁴⁸⁵Vid. la Ley Orgánica 6/2000, de 4 de octubre, por la que se autoriza la ratificación por España del Estatuto de la Corte Penal Internacional (BOE 5.10.2000), en vigor desde el 6 de octubre. Como sucede en este tipo de Leyes Orgánicas, ésta consta de un único artículo en el que se autoriza la ratificación del Estatuto, firmado por España el 18 de julio de 1998, y de una disposición adicional única en la que se señala que: «a efectos de lo previsto en el apartado b) del párrafo 1 del artículo 103 del Estatuto, España declara que en su momento, estará dispuesta a recibir personas condenadas por la Corte Penal Internacional, a condición de que la duración de la pena impuesta no exceda del máximo más elevado previsto para cualquier delito con arreglo a la legislación española». Junto a esta ley orgánica, será necesaria otra para regular la cooperación con la Corte (como se hizo en relación a los tribunales de la ex Yugoslavia y de Ruanda) y habrá que revisar el Código penal para incorporar en el mismo los crímenes de lesa Humanidad. Citado en: BLÁSQUEZ PEINADO,

*trascendencia que reviste la creación de la Corte y las importantes competencias asumidas por ella, pues el procedimiento de autorización por ley orgánica está reservado a aquellos tratados internacionales que, como sucede en el caso de los Tratados constitutivos de las Comunidades europeas y sus sucesivas reformas, operan una atribución del ejercicio de competencias derivadas de la Constitución a favor de instituciones u Organizaciones internacionales*⁴⁸⁶.

*La última fase es la de la entrada en vigor del Tratado. El Estatuto de la Corte establece en 60 el número de Estados que deben manifestar su consentimiento para la entrada en vigor del mismo*⁴⁸⁷, hecho que se produjo, el 11 de abril con la consiguiente entrada en vigor del Estatuto el 1 de julio del año 2002. (BLÁSQUEZ PEINADO, M.D. 2003:125)

M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.124.

⁴⁸⁶Vid. En este sentido, el artículo 93, párrafo primero, de la Constitución española. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.124.

⁴⁸⁷El artículo 126.1 del Estatuto de Roma prevé su entrada en vigor el primer día del mes siguiente al sexagésimo día a partir de la fecha en que se deposite en poder del Secretario General de las Naciones Unidas el sexagésimo instrumento de ratificación, aceptación, aprobación o adhesión. El Estatuto prevé, por lo tanto, para su entrada en vigor, la ratificación de al menos un tercio de los Estados existentes actualmente en la Sociedad Internacional, es decir 60 (el mismo número de Estados exigido por el artículo 308.1 de la Convención de las Naciones Unidas sobre el Derecho del Mar de 1982 para su entrada en vigor, hecho que tuvo lugar el 16 de noviembre de 1994, tras el depósito del sexagésimo instrumento de ratificación por parte de Guyana). Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.124.

4.6.2. Sistema orgánico permanente, propio e independiente.

Blásquez Peinado en este aparte investigativo hace referencia clara a lo que considera el *tercer elemento que debe poseer una organización internacional para ser considerada como tal*, y esto es un *sistema orgánico o institucional propio, permanente e independiente de sus Estados miembros*. La institucionalidad, permanencia en el tiempo e independencia es lo que permite que los organismos internacionales logren la consecución de sus objetivos y *llevar a cabo los fines y objetivos que los Estados les han asignado en el instrumento de creación*. Estos fines y objetivos, así como las necesidades derivadas del funcionamiento de cada Organización internacional van a marcar la mayor o menor complejidad de la estructura orgánica de las mismas. (BLÁSQUEZ PEINADO, M.D. 2003:124)

Teniendo en cuenta que existen diferentes Organizaciones Internacionales y *dada la variedad de Organizaciones que operan actualmente en la Sociedad internacional, es difícil hablar de una estructura orgánica adaptable a todas ellas*. Si a esto añadimos que existen distintos modos de clasificar a los órganos de las organizaciones internacionales —en virtud de su composición, de su representatividad o en virtud de la función principal que desempeñan⁴⁸⁸— la labor de establecer una estructura orgánica común a todas ellas se hace aún más complicada. (BLÁSQUEZ PEINADO, M.D. 2003:124)

⁴⁸⁸Vid. en este sentido, SOBRINO HEREDIA, J.M. en DIEZ DE VELASCO, M. Las Organizaciones Internacionales. Duodécima edición. Madrid, 2002, pág. 108 y ss. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.124.

Frente a los órganos que componen las organizaciones internacionales, la doctrina ha realizado una clasificación según la función desempeñada y el autor en cita lo ha explicado así:

Partiendo de una clasificación de los órganos en razón de la función que desempeñan dentro de la propia Organización internacional, la doctrina señala la existencia de órganos deliberantes, órganos de decisión, órganos administrativos, órganos de control —ya sea jurídico, político o financiero— y órganos consultivos. Este esquema, perfectamente aplicable a organizaciones internacionales como la ONU, el Consejo de Europa o la Unión Europea, difícilmente encaja en una institución como la Corte Penal Internacional. (BLÁSQUEZ PEINADO, M.D. 2003:125)

Ahora frente al cumplimiento de este tercer elemento dentro de la organización de la Corte Penal Internacional –institucionalidad, permanencia e independencia, el autor en cita ha manifestado:

“El sistema orgánico de la Corte viene condicionado, si cabe más que en ninguna otra Organización internacional, por la finalidad que ésta tiene asignada: ejercer jurisdicción sobre personas respecto de los crímenes más graves de trascendencia internacional⁴⁸⁹. No encontraremos en ella órganos de naturaleza deliberante, decisoria, consultiva, administrativa o de control jurídico al estilo de los que encontramos en las restantes Organizaciones internacionales. Sus

⁴⁸⁹Así se establece en el artículo Iº del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.126.

órganos son, en un sentido amplio, de naturaleza jurisdiccional porque ella es, en sí misma, un ente de carácter jurisdiccional.” (BLÁSQUEZ PEINADO, M.D. 2003 P. 128)

4.6.3. Autonomía jurídica de la Corte Penal Internacional.

En este momento investigativo tenemos como función determinar el cuarto elemento que compone la actividad y desarrollo de las funciones de las Organizaciones internacionales y que debe ser completamente aplicable a la Corte Penal Internacional, con el objetivo de que pueda ser esta como órgano de justicia universal, la encargada de la persecución de los ciberdelitos.

Tenemos entonces el planteamiento realizado por Blásquez Peinado, así:

“El cuarto y último elemento caracterizador de las Organizaciones Internacionales, al que el Tribunal Internacional de Justicia se ha referido repetidamente en su jurisprudencia, es la autonomía jurídica⁴⁹⁰. Las Organizaciones Internacionales poseen, para el cumplimiento de los fines que le han sido asignados, una personalidad jurídica distinta de la de sus Estados miembros. Sus actos se imputan a la Organización

⁴⁹⁰Vid. en este sentido el Dictamen del TU de 8 de julio de 1996, sobre la licitud de la utilización de las armas nucleares por un Estado en un conflicto armado, donde el Tribunal señala que: «les actes constitutifs d'organisations internationales sont aussi des traits d'un type particulier, ils ont pour objet de créer des sujets de droit nouveaux, dotés d'une certaine autonomie, auxquels les parties confient pour tâche la réalisation des buts communs....» CU *Recudí* 1996, parágrafo 19, pág. 9. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach. P.131.

como ente propio, autónomo e independiente, y no a los Estados que la componen.

La personalidad jurídica de las Organizaciones Internacionales es indicativa de su capacidad para ser titulares de derechos y obligaciones, tanto en las relaciones con otros sujetos del Derecho Internacional —en cuyo caso nos encontramos ante la personalidad jurídica internacional—, como cuando actúa en el ejercicio de sus funciones en el territorio de sus Estados, es decir, ejerciendo su personalidad jurídica interna. La personalidad jurídica no tiene el mismo alcance en todas las Organizaciones internacionales. La extensión de sus derechos y obligaciones depende de lo que se haya establecido en el instrumento constitutivo de cada Organización”. (BLÁSQUEZ PEINADO, M.D. 2003:125)

Vemos entonces según el planteamiento anterior que una organización internacional debe tener una personalidad jurídica diferente a la de los Estados miembros y en el caso que hemos planteado para la Corte Penal Internacional como órgano para la persecución de ciberdelitos, es precisamente este elemento el que le permite crear un ius puniendi universal que desplace al estatal para la búsqueda de justicia cuando se cometen estos delitos.

Ya específicamente frente a la personalidad jurídica de la Corte Penal Internacional, el autor en cita ha realizado el siguiente análisis:

“El Estatuto de Roma reconoce personalidad jurídica a la Corte tanto en el plano internacional como en el plano interno en el artículo 4.¹⁴⁹¹.

⁴⁹¹Vid. el artículo 4.1 del Estatuto, donde se establece que: «la Corte tendrá personalidad jurídica internacional. Tendrá también la capacidad jurídica que sea necesaria para el desempeño de sus funciones y la realización de sus propósitos. Esta previsión no figuraba en

La principal manifestación de la personalidad jurídica de la Corte en el plano internacional la encontramos en su capacidad para concluir acuerdos internacionales (iuscontrahendi), ya sea con sus Estados, con otras Organizaciones internacionales o con terceros Estados⁴⁹². En cuanto a la primera categoría de acuerdos cabe mencionar el Acuerdo de Sede de la Corte Penal Internacional con los Países Bajos, Estado parte en la Corte⁴⁹³. Este instrumento jurídico, cuyos principios básicos deben ser definidos por la Comisión Preparatoria de la Corte, y que deberá ser aprobado por la Asamblea de Estados partes y firmado por el Presidente de la Corte en nombre de ésta⁴⁹⁴, se referirá a aspectos fundamentales relacionados con el funcionamiento de la Corte: la utilización de sus locales y el derecho que debe aplicarse en el interior de los mismos, la garantía del disfrute de sus privilegios e inmunidades, o la cooperación entre la Corte y el país anfitrión, por citar algunos de estos aspectos⁴⁹⁵.

el Proyecto de la CDI de 1994 y fue incorporado en la última sesión del Comité preparatorio de 1998. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.131.

⁴⁹²Dichos acuerdos estarán sometidos al Convenio de Viena sobre el derecho de los Tratados celebrados entre Estados y Organizaciones Internacionales o entre Organizaciones internacionales, abierto a la firma el 21 de marzo de 1986. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.131.

⁴⁹³Dichos acuerdos son habituales en el ámbito de las Organizaciones internacionales, así por ejemplo, el acuerdo entre la UNESCO y Francia, de 2 de julio de 1955 o el de la ONU y los EEUU de 26 de junio de 1947. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.132

⁴⁹⁴A este respecto, vid. el artículo 3.2 del Estatuto de Roma. En el momento de concluir este trabajo, la Comisión preparatoria ha elaborado un proyecto sobre los principios básicos que deberán figurar en el Acuerdo de Sede que la Corte ha de negociar con el país anfitrión. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.132

⁴⁹⁵Vid. el informe de la Comisión Preparatoria relativo al Proyecto de principios básicos del acuerdo relativo a la sede de la Corte que han de negociar la Corte y el país anfitrión, de 26

En cuanto a los acuerdos celebrados por la Corte con otras Organizaciones internacionales, cabe destacar el Acuerdo de relación de la Corte con» las Naciones Unidas⁴⁹⁶. Pese a ser una Organización autónoma, la Corte posee importantes vínculos con las Naciones Unidas y el alcance y naturaleza de dichos vínculos se definen en el mencionado acuerdo⁴⁹⁷. Como en el caso del Acuerdo de Sede,

de abril de 2002, en PCNICC/2002//Add. 1. En dicho informe la Comisión Preparatoria establece dos tipos de principios que deberán aplicarse en la preparación del Acuerdo de Sede: unos principios generales y otros de carácter específico. En relación a los primeros, se establece, entre otras cuestiones, que dicho acuerdo plasmará la naturaleza de la relación especial entre la Corte y el país anfitrión, que deberá proveer a la independencia de la Corte y a su estabilidad a largo plazo, que deberá facilitar el funcionamiento eficiente y sin trabas de la Corte, que deberá garantizar que la Corte goce de privilegios e inmunidades y trato no menos favorable que los acordados a cualquier organización o tribunal internacionales situados en el país anfitrión, etc. En relación a los principios específicos que se deberán aplicar al Acuerdo de Sede, el informe de la Comisión Preparatoria se refiere a distintas cuestiones relacionadas con la personalidad jurídica de la Corte, con los locales de la Corte (así, por ejemplo, en caso de incendio u otra emergencia, se presume el consentimiento de la Corte para que las autoridades competentes del país anfitrión realicen la entrada necesaria en sus locales y salvo que se disponga otra cosa, en los locales de la Corte se aplica el derecho interno del país anfitrión), con los privilegios e inmunidades de la Corte (así, por ejemplo, el derecho de la Corte a enarbolar su pabellón y exhibir su emblema y distintivos en sus locales y en los vehículos u otros medios de transporte que utilice con fines oficiales, el derecho a que la Corte, sus bienes, fondos y haberes gocen, dondequiera y en poder de quienquiera que se hallen, de inmunidad de jurisdicción en todas sus formas o la exención de impuestos sobre las compras de bienes, artículos o servicios para su uso oficial), con los visados (así, la necesidad de tramitar con la mayor celeridad posible y sin cargo las solicitudes de visado de las personas que intervengan en las actuaciones ante la Corte), con la cooperación entre la Corte y el País anfitrión (así, la necesidad de que la Corte coopere en todo momento con las autoridades competentes del país anfitrión a fin de facilitar el buen funcionamiento de la justicia e impedir el abuso de los privilegios e inmunidades concedidos en virtud del acuerdo y también la necesidad de que las autoridades del país anfitrión adopten medidas eficaces para garantizar la seguridad y protección de las personas mencionadas en el acuerdo) y con el arreglo de controversias. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.132

⁴⁹⁶Dicho acuerdo se prevé en el artículo 2 del Estatuto de Roma. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.133.

⁴⁹⁷A propósito de las relaciones entre la Corte Penal Internacional y las Naciones Unidas, vid. el trabajo del profesor Cardona Lloréns, en esta obra colectiva. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.133.

también éste debe ser elaborado por la Comisión Preparatoria, aprobado por la Asamblea de Estados Partes y concluido por el Presidente en nombre de la Corte. Actualmente, dicho Acuerdo está en fase de proyecto, a la espera de su aprobación por la Asamblea de Estados partes⁴⁹⁸. El proyecto de Acuerdo parte de la conexión existente entre los Propósitos y Principios de la Carta de las Naciones Unidas y los objetivos de la Corte Penal Internacional (el mantenimiento de la Paz y la Seguridad internacionales)⁴⁹⁹ y establece un sistema de relaciones en beneficio mutuo con la intención de facilitar el desempeño de las funciones respectivas de las Naciones Unidas y de la Corte⁵⁰⁰.

⁴⁹⁸Vid. el Proyecto de Acuerdo de relación entre la Corte y las Naciones Unidas, de 9 de agosto de 2000 en PCNICC/2001/Add.I de 8.1.2002. El proyecto de acuerdo consta de 24 artículos distribuidos en 4 partes: 1ª) disposiciones generales, 2ª) relaciones institucionales, 3ª) cooperación y asistencia judicial, y 4ª) disposiciones finales. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.133.

⁴⁹⁹Vid. los tres primeros párrafos del Preámbulo del Proyecto de acuerdo de relación entre la Corte y las Naciones Unidas, donde se reafirman dichos propósitos y principios. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.133.

⁵⁰⁰Así, en las disposiciones generales se establece un reconocimiento mutuo de las labores que ambas realizan y un compromiso de respetar su condición y su mandato respectivos (artículo 2) y la Corte y las NU convienen en establecer una cooperación sobre asuntos de interés común (artículo 3). En el capítulo relativo a las relaciones institucionales, se establece que la Corte podrá asistir a la Asamblea General de las NU y participar en sus trabajos en calidad de observadora y, a la inversa, las Naciones Unidas estarán permanentemente invitadas a asistir a las audiencias públicas de las Salas de la Corte que se refieran a causas de interés para la Organización. Ambas deberán, asimismo, intercambiarse información y documentos de interés mutuo, intercambio que se llevará a cabo entre el Secretario General de las Naciones Unidas y el Secretario de la Corte (artículo 5). La Corte podrá proponer temas para su examen por las Naciones Unidas (artículo 7). Se establece también una cooperación en cuestiones administrativas (utilización de instalaciones, personal y servicios) (artículos 9 y 10). El proyecto de acuerdo establece igualmente disposiciones relativas al uso del *laissez passer* de las Naciones Unidas por parte de los Magistrados, el Fiscal, el Secretario, y el personal de ambos, como documento de viaje válido cuando ello esté reconocido por los Estados (artículo 12). Se establece, por último, una cooperación y asistencia judicial entre las Naciones Unidas y la Corte, en caso de que un funcionario de Naciones Unidas deba prestar testimonio ante la Corte (artículo 16), entre el Consejo de Seguridad de las Naciones Unidas y la Corte (artículo 17) y entre las Naciones Unidas y el Fiscal (artículo 18). Por último, y ya en el capítulo de las disposiciones finales, las Naciones Unidas y la Corte convienen en solucionar toda controversia relativa a la interpretación del acuerdo por medios apropiados

El Estatuto prevé, por último, la capacidad de la Corte para concluir acuerdos con terceros Estados —Estados no partes en el Estatuto— a fin de que éstos presten asistencia y cooperen con la Corte, en los términos en que los Estados que sí son partes están obligados a cooperar. Si concluido dicho acuerdo, el Estado en cuestión se negase a cooperar, la Corte informará de ello a la Asamblea de Estados Partes o al Consejo de Seguridad si éste le hubiese sometido el asunto⁵⁰¹.”
 BLÁSQUEZ PEINADO, M.D. (2003:134)

4.7. La Corte Penal Internacional en el marco de la creación del orden internacional en materia de mantenimiento de la Paz del siglo XXI.

Para CARDONA LLORENS⁵⁰², la creación y funcionamiento de la Corte Penal Internacional tiene relación directa con la búsqueda y mantenimiento de la Paz en el siglo XXI.

Frente a los desarrollos tecnológicos actuales ha sido imposible crear un punto de encuentro entre los avances informáticos, su utilización en la

(artículo 22), y se prevé la aprobación del acuerdo por parte de la Asamblea General de NU y de la Asamblea de Estados Partes de la Corte y la fecha de su entrada en vigor (artículo 24). Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.133.

⁵⁰¹Vid. en este sentido, el artículo 87.5. del Estatuto. Citado en: BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P.134.

⁵⁰² CARDONA LLORENS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 94.

sociedad, sus consecuencias jurídicas y su asimilación dentro de los sistemas romano-germánicos y de los de derecho consuetudinario.

Así mismo el autor en cita manifiesta que como es sabido, la comunidad internacional ha vivido un cambio de siglo muy convulso. Durante casi cincuenta años el orden internacional estuvo basado en la Carta de las Naciones Unidas adaptada a una sociedad internacional dividida tanto ideológica como económicamente. (CARDONA LLORENS, J. 2003:89)⁵⁰³

La creación y funcionamiento de la Corte Penal Internacional evidencia, según CARDONA LLORENS, que en *los últimos quince años del siglo XX van a ver (sic) modificaciones de la sociedad internacional muy significativas que van a marcar el fin de una etapa y el inicio de otra en la evolución no sólo de la sociedad internacional, sino también del Derecho internacional contemporáneo, pues esos cambios sociales van a reflejarse (o se están reflejando) de modo significativo en la configuración del orden relativo al mantenimiento de la paz y la seguridad internacionales.* (CARDONA LLORENS, J. 2003:89) Lo anterior se relaciona directamente con los objetivos y funciones de la Corte, empezando a dar luces frente a los presupuestos de justicia universal.

Adicionalmente el autor en cita ha planteado de forma categórica que *tras una etapa histórica en la que la práctica de los Estados parecía inclinarse por iniciar un camino de aceptación de la jurisdicción universal con el fin de luchar contra la impunidad de los autores de los mayores crímenes contra la humanidad, la evolución más reciente de la jurisprudencia internacional, ya entrados en el siglo XXI, así como de la práctica de los mismos Estado que*

⁵⁰³ CARDONA LLORENS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 94.

habían intentado ampliar su jurisdicción en los últimos años del siglo pasado, va a iniciar un camino contrario, recortando de modo drástico la vía expansiva de las jurisdicciones nacionales y dando, por tanto, una especial relevancia a la jurisdicción penal internacional de la CPI en el marco del nuevo orden del siglo XXI. (CARDONA LLORENS, J. 2003:90)⁵⁰⁴

4.7.1. Tendencias sociales recientes en el marco de la configuración de un nuevo mantenimiento de la paz y la seguridad internacionales

Para lograr adentrarnos en el estudio de la configuración que se dio a finales del siglo XX del nuevo mantenimiento de la paz y la seguridad mundial y que dio como resultado la creación de la Corte Penal Internacional, es necesario analizar dos factores que Cardona Llorens ha planteado, así:

“Los principales factores sociales que, en mi opinión, van a marcar la evolución de la sociedad internacional en este cambio de siglo son, fundamentalmente, dos: el fin de la guerra fría —con la consiguiente desaparición del sistema de equilibrio bipolar y la pretensión de configurar un nuevo orden político con una sola superpotencia hegemónica— y el denominado proceso de globalización.

a) El fin de la guerra fría va a suponer una nueva situación en la sociedad internacional que, aunque no supone un cambio radical de sistema, si va a influir sustancialmente en la configuración del mismo. La nueva situación provocada por el fin de la bipolaridad

⁵⁰⁴ CARDONA LLORENS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 94.

intentará ser cubierta de formas distintas e, incluso, antagónicas. Así, frente a tendencias imperialistas basadas en una sola superpotencia, van a cobrar también gran fuerza otras concepciones tendentes, bien al reforzamiento de estructuras regionales, bien al multilateralismo en la gestión de intereses colectivos.

b) La segunda de las tendencias sociales de este final del siglo XX a la que antes hacía referencia es el denominado proceso de globalización o mundialización. Este proceso supone un nuevo contexto y un nuevo cauce para la actuación de los miembros de la sociedad internacional.

Es precisamente esta segunda situación de carácter universal la que nos genera la relación necesaria entre la Corte Penal Internacional y la investigación, juzgamiento y sanción de los Ciberdelitos en búsqueda de una justicia universal. El proceso de globalización, como se explicó en el capítulo primero de la presente investigación ha sido nuestro punto de partida para determinar que los Estados deben, en casos como los de comisión de delitos informáticos, renunciar a su *ius puniendi* estatal, previa entrega de esta competencia a una Organización Internacional para que ejerza la respectiva jurisdicción.

Frente a este presupuesto se hace importante revisar los planteamientos de Cardona Llorenes, en el siguiente sentido:

“Como señalaba el Secretario general de las Naciones Unidas en su informe del Milenio⁵⁰⁵, cuando se fundaron las Naciones Unidas en 1945 las dos terceras partes de los actuales Miembros no eran Estados soberanos, sino que eran territorios sometidos a dominación colonial; la población total del planeta era de menos de 2.500 millones; las barreras comerciales eran elevadas, las corrientes comerciales minúsculas y se ejercía un firme control sobre el capital; la mayor parte de las grandes empresas funcionaban en un solo país y producían para su mercado nacional; el costo de las llamadas telefónicas transoceánicas era prohibitivo para el ciudadano medio; la producción anual de acero era un símbolopreciado de proeza económica nacional; se acababa de construir el primer ordenador del mundo, el cual ocupaba una amplia habitación, estaba dotado de 18.000 tubos electrónicos y medio millón de juntas de soldadura y para cada nueva tarea había que reconfigurar el cableado; la ecología era un tema confinado al estudio de la biología y ni en la ciencia-ficción se habrían encontrado referencias al ciberespacio.

Medio siglo después, aunque aún queda algún enclave colonial, la mayor parte de los pueblos han ejercido su derecho a la libre determinación; la población del planeta llegó antes de terminar el siglo XX a los 6.000 millones de habitantes; las exportaciones mundiales se han disparado desde 1950, incluso si se tiene en cuenta la inflación; las inversiones extranjeras han aumentado aún más rápidamente; las ventas de las multinacionales superan a las exportaciones mundiales por un margen cada vez mayor; las corrientes de divisas han aumentado de 15.000 millones de dólares diarios en 1973, cuando se

⁵⁰⁵A/54/2000. Citado en: CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 94.

derrumbó el régimen de los tipos de cambio fijos, a más de 1,5 billones de dólares; la reciente adquisición de una empresa transnacional de telecomunicaciones creó una compañía cuyo valor en el mercado supera el PIB de casi la mitad de los miembros de las Naciones Unidas juntos; hoy día los delegados de la Asamblea general de las Naciones Unidas que tengan prisa pueden cruzar el Atlántico en menos de 4 horas y, si lo desean, negociar sus asuntos de Estado en Internet o por teléfono durante el viaje.

Este proceso de mundialización se deriva de la revolución tecnológica y del impulso del modelo de economía de mercado que se impone con fuerza en los intercambios desde el fin de la guerra fría. La mundialización se ha hecho posible por el desmantelamiento progresivo de las barreras que obstaculizan el comercio y la movilidad del capital, además de los avances tecnológicos y la disminución constante de los costes de los transportes, las comunicaciones y los ordenadores.

La lógica aglutinante de este proceso parece inexorable. Sus beneficios en términos teóricos, evidentes: un crecimiento económico más rápido, niveles de vida más elevados, el aceleramiento de las innovaciones y la difusión de las tecnologías y las técnicas de gestión, y nuevas oportunidades económicas tanto para las personas como para los países.

¿Por qué entonces está empezando a haber una reacción contraria a la mundialización? Pocas personas, grupos o gobiernos se oponen a la mundialización en sí. Protestan contra sus disparidades. En primer lugar, los beneficios y oportunidades que ofrece siguen concentrados en un número muy pequeño de países y se reparten entre ellos de

manera desigual. En segundo lugar, en los últimos tiempos ha surgido un desequilibrio, puesto que se han elaborado sólidas normas que facilitan la expansión de los mercados pero no se han apoyado suficientemente objetivos sociales igualmente válidos (normas laborales, sobre medio ambiente, derechos humanos o la reducción de la pobreza). (CARDONA LLORENS, J. 2003:92)”

El autor en cita, se ha encargado de realizar el análisis del proceso de mundialización que se pretende llevar a cabo a través de la adhesión al Estatuto de Roma y del funcionamiento de la Corte Penal Internacional.

La citada mundialización de la que habla el doctrinante Español –referida a la globalización- es nuestro punto de partida para la configuración del principio de justicia universal, que consideramos debe ser aplicado a la protección de la información y los datos, que con los avances tecnológicos del momento y los móviles sociales actuales, debe ser considerada como derecho humano y fundamental.

En este sentido dijo el autor en cita:

“En términos generales, para muchas personas este proceso ha llegado a suponer mayor vulnerabilidad ante fuerzas imprevisibles que pueden provocar inestabilidad económica y trastornos sociales. Cada vez existe más temor de que la mundialización acabe siendo uniformización y amenace tanto a los modelos culturales como a la propia soberanía de los Estados. Si bien la mundialización ofrece grandes posibilidades, sus beneficios se distribuyen injustamente, al igual que sus costes. La mundialización debería ser plenamente equitativa. No debería generar ganadores y perdedores. Debería suponer algo más que la ampliación de los mercados. No se puede

separar la esfera económica del entramado más complejo de la vida social y política y dejar que siga su propia trayectoria. La economía mundial debe estar cimentada más sólidamente en valores compartidos, debe promover objetivos sociales más amplios y que den cabida a todos. Estos objetivos más amplios son la democracia, el desarrollo y el respeto de los derechos humanos⁵⁰⁶.

Pero, además, este proceso ha tenido y está teniendo consecuencias importantes en la evolución del Derecho Internacional del presente y sobre todo puede tenerlo en el futuro. Como ha sido señalado, «en esencia, es susceptible de afectar la posición tradicional del Estado soberano en este ordenamiento jurídico, dado que de un lado, su independencia para adoptar decisiones disminuye ante la realidad de una creciente interdependencia económica y tecnológica, respecto de los restantes Estados. De otro lado, porque el impulso tanto de los intercambios económicos como de las comunicaciones desborda el marco tradicional de la soberanía, es decir las fronteras del Estado, y por tanto se menoscaba la capacidad real de éste para regular esos fenómenos. Lo que supone, en correspondencia, una creciente debilidad del Estado para llevar a cabo funciones tradicionales de protección de un grupo humano tanto en el interior como frente a amenazas exteriores»⁵⁰⁷.

⁵⁰⁶Ver: CARDONA LLORENS, J. y SANZA CABALLERO, S.: «La democracia, el desarrollo y los derechos humanos como fundamento de la paz», en *Cultura de paz y medidas para garantizarla*, Valencia, 2001, pág. 110. Citado en: CARDONA LLORENS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 96.

⁵⁰⁷GONZÁLEZ CAMPOS et al.: *Curso de Derecho Internacional Público*, T ed. Madrid, 2002, pág. 72. Citado en: CARDONA LLORENS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 96.

De esta forma, el Derecho internacional contemporáneo, además de tener que acomodar sus reglas relativas al comercio internacional, verá desestabilizadas algunas de sus reglas más clásicas y tendrá que plantearse nuevos ámbitos de regulación y nuevos mecanismos de cooperación.

*Y de la misma forma que antes situábamos la creación de la **CPI** en el contexto de la realidad social provocada por la guerra fría, pienso que también debe ser analizada en el marco del proceso social generado por la mundialización o globalización. ¿Cómo justificar la creación de un mecanismo tan riguroso, poderoso jurídicamente y eficaz como es el Órgano de Solución de Diferencias en el marco de la OMC junto a la inexistencia de un Tribunal con competencia ante los mayores crímenes contra la Humanidad.*

*La **CPI** se enmarca en esa tendencia de dar una cara humana a la mundialización, de aprovechar los beneficios del proceso para el logro de una sociedad más justa, más equilibrada, en la que el ser humano y no el beneficio económico sea el centro de atención. Tal vez este sea el motivo de que los Estados Unidos sean el mayor enemigo declarado de la CPI, aunque ni los poderes otorgados a la CPI, ni los medios para garantizar sus decisiones, ni la eficacia prevista del sistema puedan compararse a los del **OSD** de la OMC (fuertemente defendido por los Estados Unidos).*

En todo caso, en mi opinión, es en el marco de estas tendencias sociales que intentan configurar el nuevo orden internacional en el que hay que contemplar no sólo la creación de la CPI sino la evolución de los valores que gira a su alrededor. El proceso de globalización influye en gran medida en la configuración del orden internacional del

mantenimiento de la paz y la seguridad internacionales en el siglo XXI. Este proceso está implicando que junto a factores positivos y al desarrollo de nuevos valores (derechos humanos, democracia y un desarrollo producto de la economía de mercado) en los que se enmarca la creación de la CPI, el fenómeno de la mundialización y de la interdependencia mutua de los Estados esté mostrando también su faz más amarga y haciéndonos olvidar su cara amable.

Al mismo tiempo, este mundo resulta menos estable que en el pasado, es sacudido por convulsiones que se producen ya no tanto entre Estados sino en su seno (golpes de Estado, nacionalismos exacerbados y violentos, odio racial y étnico, búsqueda de nuevas identidades excluyentes, intolerancia y fundamentalismo religioso, terrorismo, etc) y que están provocando la realización de los mayores crímenes que ha conocido la Humanidad.

El mundo actual se mueve entre estas dos paradojas: la búsqueda y el anhelo de una cultura de la paz basada en el fomento y las sinergias propias de la democracia, el desarrollo y los derechos humanos y el hecho fácilmente constatable del crecimiento de conflictos armados internos y nuevos riesgos para la seguridad internacional a los que la sociedad internacional debe hacer frente pese a la denodada resistencia de los Estados con argumentos basados en el respeto de su soberanía.

La lucha contra la impunidad, ya sea a través de la vis expansiva de la jurisdicción universal de los Estados o de la creación de jurisdicciones penales internacionales, se enmarca en esas tendencias.” (CARDONA LLORÉNS, J. 2003:98)⁵⁰⁸

⁵⁰⁸ CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE

4.7.2. Jurisdicción universal de los Estados versus jurisdicción penal internacional institucionalizada.

El nacimiento de la Corte Penal Internacional, surge dentro de la necesidad de los Estados y más aun de los asociados por continuar la lucha contra la impunidad y buscar justicia ante las situaciones que caían en el vacío legislativo de los Tribunales de justicia internacionales que existían antes de la Corte Penal Internacional.

Entre esas situaciones se encontraba la de inmunidad total que poseían los jefes de gobierno o altos mandos de los mismos y en este sentido se ha manifestado Cardona Llorens, así:

“Como es sabido, uno de los factores fundamentales que provoca la impunidad de los grandes criminales contra la Humanidad es su condición oficial de Jefe de Estado, presidente de Gobierno o alto cargo del Gobierno o, en su caso, su condición de antiguo titular de uno de esos cargos durante la ejecución de los crímenes de los que es acusado. La inmunidad absoluta en materia penal, tradicionalmente reconocida por el Derecho Internacional a los Jefes de Estado, Presidentes de Gobierno y Ministro de Asuntos Exteriores extranjeros se convertía, en estos casos, en verdadera causa de impunidad.

Para evitar dicha impunidad, fueron varios los Estados que iniciaron una práctica, que empezó a consolidarse a finales del siglo XX, conforme con la cual se limitaban las inmunidades de estas personas en dos sentidos convergentes: a) tanto una vez perdida su condición

de alto cargo como, b) en ocasiones extraordinarias, incluso durante su mandato.

- a) Así, en primer lugar, las legislaciones estatales y, sobre todo, los tribunales internos de los Estados van a empezar a modificar, a través de una práctica que empieza a generalizarse y una opinión *iuris* cada vez más consolidada y fundamentada, las reglas relativas a la inmunidad de los antiguos Jefes de Estado, presidentes de gobierno o ministros de asuntos exteriores extranjeros.

Conforme con dicha tendencia normativa, las inmunidades de las que gozan estas personas duran exclusivamente mientras permanecen en el cargo, de forma que, en la medida en que los tribunales internos de un Estado sean competentes, un antiguo jefe de Estado o de gobierno puede ser juzgado, no sólo por los hechos que hubiera realizado antes o después de ocupar dicho cargo, sino también por los hechos realizados durante su mandato siempre que fueran crímenes contra la humanidad.

En este sentido puede citarse como precedentes el asunto Pinochet, en el que frente a la pretensión de sus abogados de que, como antiguo Jefe de Estado chileno, Augusto Pinochet Ugarte gozaba de inmunidad ante los tribunales extranjeros, la Cámara de los Lores británica tuvo ocasión de recordar que actos como los cometidos por el acusado en modo alguno cabía incluirlos en el desempeño normal de la más alta magistratura de un Estado⁵⁰⁹

⁵⁰⁹Vide: House of Lords: Sentencia de 24 de marzo de 1999: *Regina v. Bartle and the Commissioner of Pólice for the Metrópolis and Other (Appellants), Ex Parte Pinochet (Respondent) (On Appeal from a Divisional Court of the Queen's Bench División)*; *Regina v. Evans and Another and the Commissioner of Pólice for the Metrópolis and Others (Appellants), Ex Parte Pinochet (Respondent) (On Appeal from a Divisional Court of the Queen's Bench División)* (No. 3). Citado en: CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ

b) En segundo lugar, en algunos casos excepcionales, se llega a considerar que incluso ocupando el cargo de jefe del Estado o de gobierno, existen determinados crímenes contra la humanidad ante los que no puede alegarse la inmunidad absoluta.

Esta situación, insisto que excepcional, no está sin embargo exenta de precedentes. Así, puede citarse como precedente en este sentido la sentencia de 13 de marzo de 2001 del Tribunal de Casación francés en el asunto Khadafien la que admite implícitamente que la inmunidad de los jefes de Estado tiene límites, al afirmar que «el crimen denunciado (de terrorismo) cualquiera que sea su gravedad, no se incluye entre la excepciones al principio de inmunidad de los jefes de Estado extranjeros»⁵¹⁰ CARDONA LLORÉNS, J. (2003:99).

Está claro entonces que la aparición de la Corte Penal Internacional ha generado para los países que han adoptado y voluntariamente se han obligado a su estatuto, la garantía de que independientemente del alto rango que revista las calidades de sus jefes de Estado, sus conductas cuando atenten contra la paz, derechos humano, o seguridad nacional o internacional, son objeto de conocimiento de un tribunal de justicia internacional.

Más específicamente lo ha explicado el autor en cita, cuando dice:

COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 99.

⁵¹⁰Chambre de Cassation Crim., sections réunies, S.O.S. *Attentatset as, (affaire Khadafi)* (texto en R.G.D.I.P, pág. 474). Citado en: CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 99.

“Sin duda, la competencia de este tipo de tribunales para conocer de crímenes realizados por jefes de Estado o de gobierno en ejercicio que carecen, por tanto, de cualquier tipo de inmunidad ante los mismos, está claramente consagrada. Así, en el art. 27.1 del Estatuto de Roma de la CPI se afirma la improcedencia del cargo oficial a la hora de exigir responsabilidad penal internacional o motivo para reducir la pena por la comisión de crímenes de derecho internacional:

Lo cierto es que si la CPI tuviera competencia universal para conocer de cualquier grave crimen contra la humanidad o de guerra, posiblemente no habría nada que objetar a la posición mantenida por el T.I.J. en la sentencia comentada. Pero teniendo en cuenta que dicha competencia depende de la previa aceptación por parte de cada uno de los Estados, pensamos que el giro dado a la práctica de los Estados que empezaba a consolidarse para evitar la impunidad no está claramente justificado.” CARDONA LLORÉNS, J. (2003:102)⁵¹¹

4.8. LOS TRIBUNALES ESPAÑOLES Y LAS DECISIONES DE LOS ÓRGANOS CONVENCIONALES DE DERECHOS HUMANOS EN EL ÁMBITO UNIVERSAL.

En este momento investigativo, luego de haber analizado las características de las Organizaciones Internacionales, las propias de la Corte Penal Internacional, sus ventajas frente a otros tribunales de justicia y lo conveniente para nuestro tema objeto de estudio de su creación y adhesión a través de un

⁵¹¹ CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.P. 94.

tratado internacional que solo requiere la demostración de voluntad y consentimiento de realizarlo, debemos estudiar cuales han sido las relaciones del Estado Español y sus tribunales con los órganos protectores de Derechos Humanos en el ámbito universal.

Es por la anterior razón que nos permitimos citar a Nuñez⁵¹², cuando plantea:

“No fue hasta mediados del decenio de los 70, en el pasado siglo, cuando España comenzó a ser parte de los principales Tratados de promoción y protección de los Derechos Humanos auspiciados por las Naciones Unidas⁵¹³. Estos Tratados, comenzando por el Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966 (en adelante PIDCP o «el Pacto»), crearon, como se sabe, órganos de vigilancia y supervisión del cumplimiento de las obligaciones contenidas en los mismos por parte de aquellos Estados que manifestaron su consentimiento en obligarse por los mismos⁵¹⁴.

⁵¹² NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.

⁵¹³ Así, por ejemplo, el 27 de julio de 1977 entraron en vigor para España el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Sociales, Económicos y Culturales (BOE de 30 de abril de 1977). Asimismo, el primer Protocolo facultativo del PIDCP entró en vigor para España el 25 de abril de 1985 (BOE 2 de abril de 1985); El 12 de noviembre de 1978 entró en vigor para España la Convención sobre el Estatuto de los Refugiados, de 28 de julio de 1951 (BOE de 21 de octubre de 1978); el 14 de abril de 1974 entró en vigor para España el Convenio sobre los Derechos Políticos de la Mujer de 31 de marzo de 1953 (BOE de 22 de agosto de 1974). Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas. P. 263

⁵¹⁴ Debe recordarse que el Pacto de Derechos Económicos, Sociales y Culturales de 16 de diciembre 1966 (en adelante, el Pacto), es básicamente el único tratado de Derechos Humanos adoptado en el marco de las Naciones Unidas que no crea un órgano *ad hoc* de control y supervisión de la aplicación de las obligaciones asumidas por sus Estados Partes, ya que, según su artículo 16 las funciones de supervisión del Pacto están asignadas al ECOSOC. Para llevar a cabo esta tarea, el ECOSOC, entre otras iniciativas, estableció el Comité de Derechos Sociales, Económicos y Culturales (el Comité DESC), que tiene cierto paralelismo, en cuanto a su composición, con el Comité de Derechos Humanos, pero que es un órgano subsidiario del ECOSOC y no un órgano convencional, es decir, creado por un

Desde entonces, con la reciente entrada en vigor de la flamante Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo Facultativo⁵¹⁵ y hasta que entren en vigor la Convención Internacional para la Protección de todas las Personas contra las Desapariciones Forzadas⁵¹⁶ y el Protocolo Facultativo al Pacto Internacional de Derechos Económicos, Sociales y Culturales⁵¹⁷, España ha prestado su consentimiento en obligarse por un gran número de Tratados Universales de Derechos Humanos que cuentan con un órgano de supervisión ad hoc. Todos ellos, a excepción del

tratado internacional. Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 263

⁵¹⁵ Adoptados en Nueva York el 13 de diciembre de 2006, han entrado en vigor, de forma general y para España, el 3 de mayo de 2008 (BOE de 22 de abril de 2008). Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 264

⁵¹⁶ Adoptada el 20 de diciembre de 2006, aunque 73 Estados la han firmado, sólo cuenta con 4 Estados Partes, entre los que no está aún España aunque ya se ha iniciado el trámite de la preceptiva autorización de las Cortes Generales con carácter previo a la prestación del consentimiento en obligarse por España. Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 264

⁵¹⁷ La Comisión de Derechos Humanos, creó en 2003 un Grupo de trabajo de composición abierta establecido con miras a estudiar las opciones relativas a la elaboración de un protocolo facultativo del Pacto Internacional de Derechos Económicos, Sociales y Culturales y, mediante su resolución 1/3, de 29 de junio de 2006, el Consejo de Derechos Humanos decidió prorrogar el mandato del Grupo de Trabajo por un período de dos años a fin de elaborar el citado protocolo. Sociales y Culturales. El Grupo de Trabajo se ha reunido en cinco sesiones, en 2004 (del 23 de febrero al 5 de marzo) en 2005 (del 10 al 20 de enero), en 2006 (del 6 al 16 de febrero) en 2007 (del 16 al 27 de julio) y en 2008. Dicho Grupo de Trabajo de composición abierta, presidido por la Presidenta Relatora Catarina de Albuquerque, celebró la última parte de su quinto período de sesiones del 31 de marzo al 4 de abril, en la sede de las Naciones Unidas en Ginebra, fecha en la que finalizó la redacción del Protocolo. El mismo tiene como fin establecer mecanismos de protección de los derechos contemplados en el Pacto para aquellos Estados que voluntariamente presten su consentimiento, fundamentalmente mediante la presentación, ante el Comité DESC, de denuncias individuales, ha sido adoptado por el Consejo de Derechos Humanos el 18 de junio de 2008. Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 264

Comité de los Derechos del Niño y del Comité DESC [aunque en este último caso es de esperar que por poco tiempo⁵¹⁸, tienen competencia, si el Estado Parte la acepta, para examinar comunicaciones de individuos que aleguen la violación de un derecho contemplado en el Tratado de que se trate. Los Comités, traslaman admisibilidad y el examen de dichas comunicaciones o denuncias, adoptan decisiones. Decisiones que, parece evidente a la luz del Derecho, Internacional, son obligatorias para los Estados, especialmente si resultan «condenados», sin embargo la jurisprudencia española, en especial la del Tribunal Supremo, pero también la del Tribunal Constitucional, no parece, a veces, considerarlo así, a la vista de las reiteradas Sentencias.» NÚÑEZ, P. T., (2009:264)

Lo anteriormente planteado nos lleva a la necesidad argumentativa de plantear, según los estudios de Núñez, las tres corrientes que surgen de la actividad de la administración de justicia española en concordancia con las Organizaciones Internacionales que ejercen justicia de carácter universal, así:

⁵¹⁸Cabe citar, además de lo señalado en la nota anterior, que el Consejo de Derechos Humanos, mediante su Resolución 4/7, de 30 de marzo de 2007 (A/HRC/ RES/4/7), sobre la «Modificación de la condición jurídica del Comité de Derechos Económicos, Sociales y Culturales» decidió iniciar un proceso «de conformidad con el derecho internacional y, en particular, el derecho de los tratados internacionales» que concluya en la modificación de la condición jurídica del Comité de Derechos Económicos, Sociales y Culturales y que lo equipare a todos los demás órganos de supervisión de tratados. Para ello, el Consejo de Derechos Humanos pidió al Comité de Derechos Económicos, Sociales y Culturales que elabore un informe en que se esbozen las opiniones, propuestas y recomendaciones sobre esta cuestión, solicitando, asimismo, a la Oficina de la Alta Comisionada para los Derechos Humanos, la obtención de opiniones, tanto de los Estados como de otros actores involucrados en este asunto, junto con la opinión de la Oficina de Asuntos Jurídicos de las Naciones Unidas. Se solicita, en definitiva, la valoración general sobre la pertinencia de llevar a cabo un proceso de transformación de un órgano subsidiario del ECOSOC y por lo tanto no convencional en sentido estricto, en un órgano independiente y directamente conectado al tratado de cuya supervisión se encarga, es decir, al Pacto de Derechos Económicos, Sociales y Culturales que seguiría el modelo del Comité de Derechos Humanos, creado por el PIDCP. Citado en: NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas. P. 264

“Tres vertientes merecen la pena ser examinadas en el análisis de la labor de los jueces y tribunales españoles frente a las decisiones de los órganos convencionales universales de protección de derechos humanos que operan en el ámbito de las Naciones Unidas.

En primer lugar, resulta procedente realizar una breve revisión de las Decisiones del Comité de Derechos Humanos sobre el incumplimiento por parte del sistema judicial español del Derecho a la Doble instancia penal que reconoce el Pacto Internacional de Derechos Civiles y Políticos y, a su vez, la valoración por parte de la jurisprudencia española de estas decisiones.

La segunda vertiente consistirá en un breve análisis de la interpretación y valoración que la jurisprudencia española ha realizado sobre la naturaleza jurídica de las decisiones emanadas de los órganos internacionales de base convencional de protección de derechos humanos auspiciados por las Naciones Unidas.

Finalmente, y al hilo de lo anterior, merece la pena dedicar unas líneas al examen de la naturaleza jurídica que tienen la solicitud de adopción de medidas provisionales que los mencionados órganos pueden realizar con el fin de evitar vulneraciones inminentes (o mayores) de los derechos humanos que pretenden proteger.” NÚÑEZ, P. T., (2009:265)

4.9. La interpretación por parte de la Jurisprudencia española de las decisiones de los órganos convencionales de supervisión de Derechos Humanos.

En este aparte de la presente tesis nos proponemos a realizar un estudio frente a lo que ha planteado y desarrollado la jurisprudencia española en relación a decisiones de derechos humanos adoptadas por organismos internacionales, en este sentido el autor en cita anterior ha planteado:

“Se pretende ahora examinar cuál es la interpretación y, por tanto, la valoración que la jurisprudencia española realiza sobre las Decisiones del Comité de Derechos Humanos y, por extensión, de las adoptadas por otros órganos, de base convencional, de protección y promoción de los Derechos Humanos auspiciados por las Naciones Unidas.

Por lo que respecta a la naturaleza jurídica, tanto de las decisiones, como de las solicitudes de adopción de medidas provisionales por parte del Comité de Derechos Humanos, que serán objeto de atención más adelante, y de otros órganos convencionales de control de Derechos Humanos, ha de recordarse, en primer lugar, y por obvio que pueda parecer, que el Derecho Internacional establece claramente que «[t]odo tratado en vigor obliga a las partes y debe ser cumplido por ellas de buena fe», según dispone art. 26 de la Convención de Viena sobre el Derecho de los Tratados, de la que España es Parte. A su vez, la Constitución española, en su art. 96.1, afirma que «[l]os tratados internacionales, válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Sus disposiciones sólo podrán ser derogadas, modificadas o suspendidas en la forma prevista en los propios tratados o de acuerdo con las normas generales de Derecho internacional».

No obstante todo lo anterior, el Tribunal Supremo español ha manifestado, en reiteradas ocasiones, que el Comité de Derechos Humanos es un órgano «político» que no tiene carácter jurisdiccional, cuya importancia está en influir en los órganos de los Estados Partes, pero cuyos dictámenes carecen de carácter ejecutivo. Esta doctrina puede verse reflejada en numerosas Sentencias, así en la Sentencia 141/2005, de 11 de febrero de 2005, de la Sala de lo Penal del Tribunal Supremo, se argumenta lo siguiente:

«El art. 14.5 del Pacto de Nueva York de 1966 ha originado ya varias resoluciones del mencionado comité de la ONU, órgano político de orden internacional encargado de velar por el cumplimiento de tal pacto (...).

Con lo expuesto queremos poner de relieve que el mencionado Comité de Derechos Humanos de la ONU no tiene carácter jurisdiccional de modo que sus resoluciones o dictámenes carecen de aptitud para crear una doctrina o precedente que pudiera vincular a esta Sala de lo Penal del Tribunal Supremo, de modo que el efecto jurídico que puede producir queda reducido a lo expuesto: esa declaración de existencia de vulneración del mencionado art. 14.5 del pacto referido y ese requerimiento para que el Estado Español, a través de sus órganos, le conteste y diga qué medidas concretas adopta en el caso correspondiente y en la legislación española para que no volviera a repetirse la citada vulneración»⁵¹⁹.» NÚÑEZ, P. T., (2009:273)

⁵¹⁹En el mismo sentido al arriba reproducido puede citarse, también, el arriba reproducido Auto del la Sala Segunda, de lo Penal, del Tribunal Supremo, de 14 de diciembre de 2001. Citado en: NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 273

Define entonces a modo de conclusión el autor en cita que *Según lo expresado, la doctrina, reiterada, de un órgano internacional al que España ha prestado su consentimiento en aceptar su competencia, mediante la ratificación, con la previa autorización del poder legislativo, del Protocolo Facultativo del Pacto*⁵²⁰, *no puede siquiera ser un precedente vinculante para el poder judicial de este mismo Estado*⁵²¹. *Este razonamiento equivaldría a sostener que nuestro poder judicial es un «reino» al que no le afectan, si no lo desea, las obligaciones internacionales asumidas por el Estado y que el resto de los poderes públicos, a cualquier nivel, debe cumplir.* NÚÑEZ, P. T., (2009:274)⁵²²

No obstante lo anterior, para Núñez existen claras diferencias entre los planteamientos del Tribunal Supremo Español y los del Tribunal Constitucional Español frente a las decisiones de Organismos Internacionales, esto se evidencia cuando cita:

⁵²⁰ El artículo 1 del Protocolo Facultativo no deja lugar a dudas: todo Estado Parte tanto del Pacto como del Protocolo «reconoce la competencia del Comité para recibir y considerar comunicaciones de individuos que se hallen bajo la jurisdicción de ese Estado y que aleguen ser víctimas de una violación, por ese Estado Parte, decualquiera de los derechos enunciados en el Pacto». Citado en: NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 273

⁵²¹ En la misma línea, y entre otros, el anteriormente citado ATS de 16 de febrero de 2004 afirmó que «como se desprende del propio contenido del Pacto y Protocolo y como señala unánimemente la doctrina, los Dictámenes del Comité no tienen valor jurídico vinculante, salvo el que quiera otorgarle el Estado afectado por la condena». Así pues, se confunde valor jurídico vinculante con fuerza ejecutiva directa. Citado en: NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 273

⁵²² NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas

“Ahora bien, hay que reconocer que, a diferencia de la jurisprudencia del Tribunal Supremo, el Tribunal Constitucional, con acierto, distingue entre «carácter jurisdiccional», «fuerza ejecutoria directa» y «obligatoriedad». Que un órgano no tenga carácter jurisdiccional y que, en consecuencia, sus decisiones no tengan ejecutoriedad⁵²³, no significa que las mismas no sean obligatorias para el Estado respecto al que se dictan. Cabe recordar que esta distinción entre obligatoriedad de un lado y ausencia de fuerza ejecutiva, de otro, ha sido ampliamente empleada por la jurisprudencia española respecto a las Sentencias del Tribunal Europeo de Derechos Humanos.

Es justo resaltar, no obstante, que el propio Tribunal Constitucional ha puesto de manifiesto, en la Sentencia anteriormente citada, que los Dictámenes del Comité de Derechos Humanos no carecen de valor jurídico:

«Ahora bien, el que los Dictámenes del Comité no sean resoluciones judiciales, no tengan fuerza ejecutoria directa y no resulte posible su equiparación con las Sentencias del Tribunal Europeo de Derechos Humanos, no implica que carezcan de todo efecto interno en la medida en que declaran la infracción de un derecho reconocido en el Pacto y que, de conformidad con la Constitución, el Pacto no sólo forma parte de nuestro Derecho interno, conforme al art. 96.1 CE, sino que además, y por lo que aquí interesa, las normas relativas a los derechos fundamentales

⁵²³Cabe recordar aquí que para la jurisprudencia española tampoco las Sentencias del Tribunal Europeo de Derechos Humanos tienen fuerza ejecutiva, sino meramente declarativa, Citado en: NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 274

y libertades públicas contenidas en la Constitución deben interpretarse de conformidad con los tratados y acuerdos internacionales sobre las mismas materias ratificados por España (art. 10.2 CE); interpretación que no puede prescindir de la que, a su vez, llevan a cabo los órganos de garantía establecidos por esos mismos tratados y acuerdos internacionales (STC 81/1989, de 8 de mayo, FJ 2)».

Así pues, para el Tribunal Constitucional, los Tratados Internacionales de los que el Estado Español es Parte sólo tienen *fuera hermenéutica*:

«Este Tribunal, desde sus primeras Sentencias, ha reconocido la importante función hermenéutica que para determinar el contenido de los derechos fundamentales tienen los tratados internacionales sobre derechos humanos ratificados por España (...), habiendo declarado expresamente que el contenido de los derechos humanos reconocidos en el Pacto constituye parte también del de los derechos fundamentales, "formando el estándar mínimo y básico de los derechos fundamentales de toda persona en el Ordenamiento jurídico español" (...).» NÚÑEZ, P. T., (2009:276)⁵²⁴

El Tribunal Constitucional Español, según sus líneas interpretativas, no considera vinculantes los instrumentos jurídicos aplicables a este Estado. Solo los tienen en cuenta como fuente interpretativa y siempre que no sean proyectados y analizados de esa manera dentro de la legislación nacional, incurriendo en lo que hemos manifestado, es el primer elemento que se debe

⁵²⁴ NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas

eliminar, la lucha por la soberanía en la aplicación del ius puniendi estatal versus el ius puniendi universal.

Esta situación la evidencia Núñez en su obra en cita, así:

“Cabe mencionar, en la línea de esta interpretación, que el TC no considera que los derechos contenidos en los Instrumentos jurídico vinculantes sean directamente aplicables en España. De acuerdo con la citada función hermenéutica, lo son sólo en la medida en que los derechos fundamentales contenidos en la Constitución Española deben interpretarse de acuerdo con ellos. Cabe citar, en este sentido, el Auto del TC de 13 de noviembre de 2000, citado en el epígrafe anterior. En él, el Tribunal Constitucional razona que la lesión de algún derecho humano reconocido en el PIDCP y acreditada por el Comité de Derechos Humanos (al Comité, sorprendentemente, en el Auto referido se le denomina en numerosas ocasiones «Comisión») supone una vulneración de los derechos fundamentales del recurrente:

«la lesión de diversos derechos humanos reconocidos en el Pacto, declarada en el Dictamen de la Comisión, puede acreditar la posible vulneración de los correspondientes derechos fundamentales del recurrente, puesto que el contenido de aquéllos constituye parte también de éstos, formando el estándar mínimo y básico de los derechos fundamentales de toda persona en el Ordenamiento jurídico español, como resulta de la circunstancia de que los tratados y acuerdos internacionales sobre Derechos Humanos sean insoslayables instrumentos hermenéuticos de los derechos fundamentales de la Constitución Española (art. 10.2 CE)».

Estas líneas no expresan un razonamiento nuevo del Tribunal Constitucional español respecto a los Tratados Internacionales de Derechos Humanos por los que se ha obligado España. Parece que los derechos contenidos en los mismos no son directamente aplicables a aquellas personas que son objeto de protección de los mismos, sino que sólo lo serán en la medida que ayuden a interpretar los Derechos Fundamentales reconocidos en la Constitución. Por los argumentos expresados al inicio de este epígrafe, no puedo sino mostrar mi desacuerdo con este razonamiento.

Así pues, queda claro, a la vista de la Jurisprudencia española sobre la cuestión, que la eficacia de las decisiones de los órganos de control creados por Tratados sobre Derechos humanos auspiciados por las naciones Unidas, se basa, principalmente, en la publicidad de las mismas. Esta interpretación no es, a mi juicio, la correcta, ya que el hecho de que tanto el Comité de Derechos humanos como otros órganos de base convencional similares, no tengan carácter jurisdiccional, no implica que sus decisiones no deban ser obligatorias para los Estados que han manifestado voluntariamente su consentimiento en obligarse por los Convenios sobre Derechos humanos que estos órganos supervisan, así como por los procedimientos de supervisión y control establecidos por ellos. En efecto, estos mecanismos convencionales no obligan más que a los Estados que voluntariamente han prestado su consentimiento en obligarse por ellos y, una vez prestado este consentimiento, deberán cumplir las obligaciones emanadas de tales tratados de buena fe. Si bien las Decisiones adoptadas por los Comités de supervisión y control de los Tratados ad hoc de Derechos humanos no son, como señala

*nuestra jurisprudencia, resoluciones judiciales con fuerza ejecutiva, España sí que está obligada por ellas*⁵²⁵.” NÚÑEZ, P. T., (2009:276)

4.9.1. Conclusiones

A modo de conclusión frente a la posición de los Tribunales españoles, que no se resisten a darle fuerza vinculante a los preceptos contenidos en tratados internacionales asumidos por el Estado Español, y que en la búsqueda inocua de mantener la soberanía desde la administración de justicia no renuncian a ninguna de sus potestades estatales, Núñez se ha manifestado, estableciendo que:

“Parece claro, a la vista de lo anterior, que los tribunales españoles se resisten a aceptar que están obligados por las decisiones de los órganos convencionales creados por Tratados internacionales sobre Derechos Humanos de carácter universal, de los que España es Parte. Órganos cuya competencia para aceptar y examinar denuncias individuales respecto a España el Estado español ha aceptado expresamente.

A pesar de ello, la jurisprudencia de estos órganos encargados de la supervisión y el control de los Tratados universales de promoción y

⁵²⁵Tal y como señaló S. Ripoll respecto al Dictamen 701/1996 de 20 de julio de 2000, cuando el Comité de Derechos Humanos recuerda que España tiene la obligación de tomar las disposiciones necesarias para que, en lo sucesivo, no ocurran violaciones parecidas, esta obligación «no deriva directamente de la decisión, ni siquiera del Protocolo Facultativo, el cual no se refiere en momento alguno a un eventual compromiso de los Estados partes de aplicar las observaciones del Comité, sino que debe situarse en el marco convencional que da origen al sistema de protección, el Pacto Internacional de Derechos Civiles y Políticos» «El Dictamen...» *Loe. Cit.* P. 474. Citado en: NÚÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Carlos R. Fernandez Liesa (Director). Tribunales Internacionales y espacio Iberoamericano. Madrid: Civitas.P. 276

protección de los Derechos Humanos acaba, más tarde que pronto, teniendo su incidencia tanto en las sentencias dictadas por los tribunales españoles como en la legislación interna que regula el sistema judicial.

No obstante, la interpretación que se sigue realizando por parte de la jurisprudencia española, tanto de las decisiones emanadas de los órganos convencionales encargados de la supervisión de los derechos contenidos en los Tratados por los que se crean, como de los mismos derechos contenidos en estos Tratados, se aleja aún de lo deseable desde el punto de vista del Derecho internacional de los Derechos Humanos. Ello es así porque a las primeras les otorga nuestra jurisprudencia una mera «naturaleza política» y a los segundos, a los derechos, sólo les reconoce valor en España en tanto los Derechos fundamentales reconocidos en la Constitución Española han de interpretarse a la luz de aquéllos, según dispone el artículo 10.2.

Pero quizá lo más sorprendente no es la peculiar interpretación del Derecho Internacional público que pueden realizar los jueces y tribunales españoles, obviando a veces la obligatoriedad de aquello a lo que un Estado ha prestado formal y, por supuesto, voluntariamente, su consentimiento en obligarse, requiriendo para ello, en estos casos, la previa autorización de las Cortes Generales en virtud de lo dispuesto en el artículo 94.1 de la Constitución Española. Sino que, además, las resoluciones judiciales españolas han llegado hasta a negarle a estos órganos convencionales de protección de los derechos humanos la facultad de interpretar las disposiciones de aquellos Tratados por los que fueron creados. (NÚÑEZ, P.T., 2009:280)

5. APLICACIÓN DE LA JUSTICIA PENAL INTERNACIONAL FRENTE A LOS DELITOS COMETIDOS EN LA CIBERSOCIEDAD.

5.1. IMPUTACIÓN Y DERECHO PENAL INTERNACIONAL

5.1.1. Imputación de comportamientos macrocriminales.

Kai Ambos en su obra *La parte general del Derecho Penal*, citando a Jager, aborda *La problemática de la imputación de comportamientos macrocriminales*. Posteriormente trata las conductas macrocriminales y su imputación en su trabajo fundamental sobre los crímenes cometidos durante el nacionalsocialismo y *había examinado estos hechos aún desde una perspectiva empírica-interdisciplinaria*,⁵²⁶ Finalmente este autor ha reflexionado concretamente sobre la "imputación individual de la conducta colectiva". (AMBOS, K., 2006 P. 148)⁵²⁷

Frente al concepto de comportamientos macrocriminales, Ambos en su obra en cita, toma los argumentos de Jager, Peters, Eichmann, Jakobs, Lampe, Naucke y Marxen y mostrando el desarrollo dogmático de este concepto, así:

*Además de Jäger, también otros autores se han ocupado de cuestiones particulares de la imputación de crímenes colectivos. Ya con anterioridad, Peters se había ocupado en relación con el proceso Eichmann de la estructura e imputación de los crímenes de masa.*⁵²⁸ *Desde una perspectiva exclusivamente de dogmática penal, Jakobs ha*

⁵²⁶ Jäger, Verbrechen (1982), passim. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵²⁷ Jäger, Makrokriminalität (1989), p. 132 ss.; el artículo respectivo fue publicado originariamente. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵²⁸ Peters, Eckart, Jb 1961, 232 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

analizado la cuestión de la repercusión de los diagnósticos psíquicos sobre el reproche de culpabilidad penal.⁵²⁹ Lampe ha intentado desarrollar un "derecho penal del sistema" (System-Strafrecht)⁵³⁰ Naucke propone una "cuarta vía de derecho penal" para luchar contra la "criminalidad reforzada por el Estado".⁵³¹ Marxen, por su parte, ha sido el primero y hasta ahora el único en esbozar puntos de partida concretos para una teoría del delito de derecho penal internacional.⁵³² (AMBOS, K., 2006 P. 148)⁵³³

Ahora, en los acápites siguientes nos dedicaremos a establecer la concepción de cada uno de los autores que Ambos ha considera importantes al determinar la imputación de crímenes colectivos.

5.1.2. Peters: primeras reflexiones sobre una imputación de crímenes colectivos.

El concepto de *Peters* frente a crímenes colectivos viene creándose desde las actuaciones realizadas en la época del Nacionalsocialismo, este autor *consideró a los crímenes del nacionalsocialismo como "algo absolutamente novedoso" no sólo debido a su carácter de crímenes de masa, sino especialmente porque ellos no se dirigieron contra el Estado y tampoco fueron perseguidos por éste (quienes se encontraban imputadas eran "justamente la*

⁵²⁹ *Jakobs*, en: Goppinger/Bresser (editores), Sozialtherapie (1982), p. 127 ss. *Lampe*, ZStW 1994, 683 ss. Existe versión en castellano en *Lampe*, Dogmática (2003), p. 97 ss. *Naucke*, Privilegierung (1996), p. 65 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵³⁰ *Marxen*, en: Lüderssen (editor), Kriminalpolitik III (1998), 220 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵³¹ *Marxen*, en: Lüderssen (editor), Kriminalpolitik III (1998), 220 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵³² Se trata de opiniones aparecidas con posterioridad a la publicación del texto original alemán e por primera vez en esta versión castellana. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵³³ AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

clase dirigente de la conducción del Estado y las fuerzas más importantes para la formación de la sociedad"). (AMBOS, K., 2006 P. 148)⁵³⁴. Así mismo Ambos expone que al servicio de estos crímenes se encontraba un aparato de poder, que garantizaba su "extensión, sistematicidad, puntualidad y perfección". (AMBOS, K., 2006 P. 149)⁵³⁵. Para Ambos, Los crímenes eran "dirigidos desde lugares alejados al hecho" por las "altas clases sociales y económicas en una posición de poder". (AMBOS, K., 2006 P. 149)⁵³⁶ de ahí mismo la conclusión de que su ejecución ocurría "de modo sistemático y meditado" y las eventuales oposiciones eran eliminadas. La característica especial de estos crímenes residiría según Peters en que "entre el momento desencadenante del hecho y el hecho mismo" se intercalaba una "reflexión", esto es, "ponderación, cálculo, previsibilidad y dominio del suceso". (AMBOS, K., 2006 P. 149)⁵³⁷

En la obra de Ambos, cuando cita a *Peters*, el segundo autor plantea la teoría del crimen ideológico, que se caracterizaría además por el gran número de víctimas y de posibles autores,⁵³⁸ arraigándose en el "entero espacio social". (AMBOS, K., 2006 P. 149)⁵³⁹ Por ello, en su opinión, se habría de partir de la "co-solidaridad de otros, innumerables, hombres", quienes sin embargo no serían automáticamente co-responsables jurídico-penalmente. Más bien, la "co-solidaridad" plantearía complejos problemas de delimitación entre la responsabilidad (solamente) moral y la que (ya) es penal. La comisión de crímenes de masa implicaría una "cadena de acción" —que conduce

⁵³⁴ . *Peters*, Eckart Jb 1961, 232. ídem, 233. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 148.

⁵³⁵ ídem. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵³⁶ ídem, 234. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵³⁷ ídem, 235. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵³⁸ ídem, 238. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵³⁹ ídem, 240. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

directamente al hecho y está en conexión con éste—, en la cual intervendrían muchas personas.⁵⁴⁰ Junto con las personas que han ideado y guiado intelectual-mente los crímenes, existirían "órganos ejecutivos con mayor o menor autorresponsabilidad".⁵⁴¹ Quien participa "dando órdenes y dirigiendo" sería, para Peters, autor, sin importar el rango que ocupa. Por el contrario, la "gran cantidad de subordinados o de participantes marginales" serían punibles como cómplices. Precisamente la intervención de un "sinnúmero de personas decentes y [normalmente] respetuosas del derecho", plantearía también la cuestión de la culpabilidad moral de todos los miembros de la sociedad. (AMBOS, K., 2006 P. 149)⁵⁴²

5.1.3. Jäger: imputación individual con conducta colectiva.

Ambos considera de gran importancia la teoría planteada por Jäger frente a imputación individual con conducta colectiva, de esta forma Jäger ha planteado en su "Studie zur nationalsozialistischen Gewaltkriminalität" (*Estudio sobre la criminalidad de poder durante el nacionalsocialismo*) que, entre otras cosas, *las repercusiones del estado de necesidad por cumplimiento de una orden sobre el reproche jurídico-penal de culpabilidad.* (AMBOS, K., 2006 P. 149)⁵⁴³ *El autor llega a la conclusión de que su importancia criminológica es "esencialmente menor" de lo que con frecuencia se supone. El receptor de la orden estaría expuesto con frecuencia a una "presión psicológica fuerte, pero no exculpante". En cambio, mayor importancia se debería asignar en su opinión al estado de necesidad subjetivo por cumplimiento de una orden (estado de necesidad putativo); el problema*

⁵⁴⁰ ídem, 240 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵⁴¹ ídem, 241. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵⁴² ídem, 245 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

⁵⁴³ Jäger, Verbrechen (1982), p. 83 ss. (158-160). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 149.

de éste sería sin embargo que no se podría demostrar empíricamente con precisión. En cuanto a la conciencia de la antijuridicidad de los autores totalitarios, Jager llega a la conclusión (AMBOS, K., 2006 P. 149)⁵⁴⁴ de que, si bien también puede ser demostrada en los hechos colectivos, "en muchos casos no se puede decir realmente cómo valoró el propio autor su conciencia de antijuridicidad". En todo caso, se llegaría a una cierta "individualización del problema", en el sentido de que la falta de conciencia de antijuridicidad no tendría por lo general sus "causas" en el contexto de la "época", sino en motivos "individuales". Por lo demás, se habría de reconocer "con bastante claridad" que los mismos criminales principales no habrían atribuido a las órdenes de exterminio "ningún significado de naturaleza jurídica, legalizante", sino que "eran absolutamente conscientes" de su antijuridicidad, aunque las hayan considerado ideológicamente justificadas. (AMBOS, K., 2006 P. 150)

El autor en cita (Jager) advierte sobre los presuntos límites del derecho penal orientado al injusto personal en caso de crímenes colectivos, sin extraer de ello, sin embargo, la consecuencia de una incompetencia jurídico-penal. Más bien, el "análisis microscópico de la conducta individual" propia del derecho penal pone en evidencia justamente "la dimensión personal del injusto colectivo" (AMBOS, K., 2006 P. 150)⁵⁴⁵.

Jäger en su dogmática también define el terror colectivo donde este concepto no puede considerarse como "simplemente una catástrofe natural", sino que se compondría "de actos individuales criminales de lo más diferentes, con frecuencia co-controlados por impulsos personales al hecho". (AMBOS, K., 2006 P. 150)

⁵⁴⁴ ídem, p. 166 ss. (324 s.). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 150.

⁵⁴⁵ Jager, KJ 1968/69, 144 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 150.

Continuando con la dogmática penal desarrollada por Jäger, encontramos que en el año 1980 Jager, en palabras de Ambos, *llamó la atención sobre dos particularidades de los "crímenes colectivos": los cambios colectivos de orientación del valor moral ligados a estos crímenes y la importancia especial de las influencias situacionales, de las condiciones externas de acción y de las fuerzas de adaptación de la dinámica de grupos. Éstas hacían difícil la "inmutabilidad individual" de estos crímenes desde el punto de vista objetivo y subjetivo, pues "el particular no puede responder por la dimensión total de los daños causados colectivamente y con frecuencia su aporte individual al resultado no puede ser aislado suficientemente". Con ello, Jager advierte también —en cuanto se conoce por primera vez— acerca de las posibles repercusiones de la comisión colectiva sobre el reproche individual de culpabilidad. Sin embargo, él sostiene que los problemas de imputación mencionados no deberían conducir "a pasar completamente por alto la dimensión individual de la conducta colectiva o a considerarla de todos modos como no esencial", sino que, por el contrario, ésta debería ser puesta en evidencia,⁵⁴⁶ pues "también los crímenes colectivos no son otra cosa que crímenes individuales en lo colectivo". (AMBOS, K. 2006:150)⁵⁴⁷ Para Jäger, definir las teorías de la justificación y la neutralización, en un momento posterior a la configuración de la conducta punible, tendría otro significado, así *Las usuales "teorías de justificación y técnicas de neutralización" luego de la comisión de tales crímenes no sólo tienen el "significado de autoexoneración a posteriori", sino que precederían a la conducta criminal, le allanarían psicológicamente el camino y de esa forma la posibilitarían*". (AMBOS, K. 2006:150)⁵⁴⁸ En este momento investigativo es cuando, *concluye**

⁵⁴⁶ Cfr. en este sentido también Jager, MschrKrim 1980, 365. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 150.

⁵⁴⁷ Jager, MschrKrim 1980, 359 s.; sobre las categorías jurídico-penales afectadas cfr. idem, en la nota 3. Sobre los grupos terroristas cfr. Jager, KrimJ 1983, 131 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 150.

⁵⁴⁸ ídem, 360 s. Con más detalles sobre las "condiciones y mecanismos de la neutralización", también Jager, Makrokriminalität (1989), p. 187 ss.; recientemente también Rotsch, wistra

Jager, "que la dimensión individual no interviene en modo irrelevante en el origen de los crímenes colectivos".(AMBOS, K. 2006:150)⁵⁴⁹

Frente a la imputación individual en crímenes denominados como colectivos, se pronunció Jäger estableciendo que:

"Los problemas de imputación individual de crímenes colectivos fueron analizados por Jager detalladamente en su monografía del año 1985, la cual sin alteraciones fue nuevamente publicada en el volumen sobre macrocriminalidad aparecido en 1989. (AMBOS, K. 2006:151)⁵⁵⁰ Ante todo, Jager advierte nuevamente sobre el problema de la imputación individual: mientras que el injusto (objetivo) de tales hechos habría de ser afirmado sin más, la culpabilidad individual sería problemática, pues se plantearía la cuestión de "si el participante individual podría ser hecho responsable personalmente en toda su extensión por acciones que forman parte de un suceso colectivo y cuyo autor es en definitiva el colectivo y no el individuo".(AMBOS, K. 2006:151)⁵⁵¹ En definitiva, Jager afirma esa cuestión y separa el análisis criminológico del problema jurídico-penal de la exculpación. (AMBOS, K. 2006:151)⁵⁵² Las transformaciones del individuo en la masa comprobadas por la psicología de masas tendrían como consecuencia, desde un punto de vista de dogmática penal, a lo más la atenuación de la pena o de la

1999, 369 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁴⁹ Jager, MschrKrim 1980, 363. Jager se pregunta en este contexto si, por ejemplo, la masacre My Lai (cfr. § 5 II. 1. vers. al.) se debería atribuir sólo a la situación especial de la guerra y a la ambigüedad de la situación jurídica o no también a la "liberación de 'tendencias criminales latentes'". Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵⁰ Jager, Makrocriminalität (1989), p. 132 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵¹ ídem, p. 133. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵² ídem, p. 136. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

culpabilidad, pero no la exclusión de la culpabilidad. Según Jager, la afirmación de responsabilidad penal se habría "impuesto claramente, si bien ligada a la exigencia de un juicio individualizante".(AMBOS, K. 2006:151)⁵⁵³ Por ello, para este autor sería un "malentendido fundamental" el interrogarse por una causa de exclusión de la culpabilidad, pues "la responsabilidad faltante en el sentido de una incapacidad de imputación y de culpabilidad de ningún modo es el obvio correlato normativo de aquel fenómeno psicológico que ha sido descrito por la psicología de masas como debilitamiento o pérdida del sentimiento de responsabilidad".(AMBOS, K. 2006:151)⁵⁵⁴ Tampoco los procesos de dinámica de grupos tendrían —en contra de la opinión de Schumacher— un efecto exculpante. (AMBOS, K. 2006:151)⁵⁵⁵ De todos modos, la característica de los crímenes colectivos sería, en su opinión, que "la conducta individual no se determina en primera línea por motivos relacionados con el hecho, sino por motivos de dinámica de grupos".(AMBOS, K. 2006:151)⁵⁵⁶ Esto podría tener efectos especialmente en el actuar en cumplimiento de una orden. (AMBOS, K. 2006:151)⁵⁵⁷

De esta forma cuando hablamos de crímenes colectivos es necesario tener en cuenta la posición de Hofstatter, quien advirtió que: *más bien en el marco de una guerra que en tiempos de paz se cumplirían órdenes que representan*

⁵⁵³ ídem, p. 136 ss. (143). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵⁴ ídem, p. 146. Expresamente contra *Le Bon* (144 ss.). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵⁵ ídem, p. 146 ss. Recientemente sobre la dinámica de grupos, también *Rotsch*, wistra 1999, 368 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵⁶ *Jager*, Makrokriminalitát (1989), p. 152. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

⁵⁵⁷ ídem, p. 164. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 151.

crímenes de guerra. (AMBOS, K. 2006:152)⁵⁵⁸ Como mecanismos de disminución de la inhibición entrarían en consideración la distancia espacial de la ejecución del hecho procurada por medio de la técnica y la distancia social. (AMBOS, K. 2006:152)⁵⁵⁹ Sin embargo, la consideración de los efectos de la dinámica de grupos en el juicio penal de culpabilidad habría sido rechazada por la dogmática penal por ser "problemática" e "ilimitada" (AMBOS, K. 2006:151)⁵⁶⁰ y solamente Jakobs se habría ocupado sustancialmente del tema (sobre esto, se volverá pronto). Desde una perspectiva empírica Jager expresa que tendría que concluirse que los efectos de la dinámica de grupos no conducirían a trastornos de la conciencia en el sentido de los § 20 y 21 del StGB- y, por consecuencia, sólo podrían ser considerados de legeferenda. (AMBOS, K. 2006:151)⁵⁶¹ Si bien es cierto, argumenta, que se podrían divisar ciertos "defectos de socialización" específicos de los grupos como "causas del delito criminológicamente significativas", por ejemplo, la sujeción al Estado o a otro colectivo, ellas no deberían ser privilegiadas, sin embargo, por la vía de la exculpación. (AMBOS, K. 2006:151)⁵⁶² En definitiva, la imputabilidad individual dependería de la medida en que se puedan reconocer "efectos y rastros de tendencias, motivos e impulsos individuales" en las acciones colectivas, esto es, pasarían a

⁵⁵⁸ ídem, p. 166. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

⁵⁵⁹ ídem, p. 166 ss., 168: la "distancia [...] neutraliza el sentimiento moral". Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

⁵⁶⁰ ídem, p. 173, especialmente con referencia a Lackner y Jakobs; cfr. también ya ídem, p. 147. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

⁵⁶¹ N. del T. El § 20 del StGB se refiere a la incapacidad de culpabilidad por perturbaciones mentales (*Schuldunfähigkeit wegen seelischer Störungen*); el § 21 StGB regula la facultad de atenuación de pena para los casos de capacidad de culpabilidad disminuida (*verminderte Schuldfähigkeit*). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

⁵⁶² ídem, p. 178 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

segundo plano los modelos de acción "ajenos de personalidad" inmanentes a la comisión colectiva del hecho. (AMBOS, K. 2006:151)⁵⁶³

Posteriormente, en el año 1995 Jager ha nuevamente clarificado su comprensión del concepto de macrocriminalidad, definiendola como "comportamientos conforme al sistema y adaptados a la situación dentro de una estructura de organización, aparato de poder u otro contexto de acción colectiva". (AMBOS, K. 2006:153)⁵⁶⁴ A través de esta concepción de la macrocriminalidad Jäger logra continuar con su convicción dogmática en la que a pesar de los conocidos problemas en cuanto a la imputabilidad de tales crímenes,⁵⁶⁵ el autor sigue aferrándose a la atribución individual de culpabilidad y se expresa en contra del "derecho penal del sistema" ("System-Straf-recht") propuesto por Lampe. Aunque se pueda sostener, argumenta Jager, que ya la pertenencia a un régimen criminal significa un injusto, tal opinión acabaría en una punibilidad fundada en la mera pertenencia a la organización, sin considerar los propios crímenes cometidos dentro de la organización. Ya por este motivo, el "regreso a las atribuciones de culpabilidad colectiva" no representaría una salida a las dificultades de la imputación individual. Las "acciones penales" de la comunidad internacional contra los regímenes ilícitos, aunque posiblemente legítimas, no tendrían "nada que ver con el derecho penal internacional, y con la pena, en el mejor de los casos, sólo compartirían el nombre". Además, ellas mismas podrían derivar sencilla y "repentinamente en un injusto macrocriminal". Tampoco la dimensión política de tales crímenes prohibiría la atribución individual de culpabilidad.

⁵⁶³ Ídem, p. 179 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 152.

⁵⁶⁴ Jager, en: Hankel/Stuby (editores), Straßgerichte (1995), p. 327, también 331. Cfr. sobre el concepto, también ya supra § 1 Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 153.

⁵⁶⁵ Jager, en: Hankel/Stuby (editores), Straßgerichte (1995), p. 329. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 153.

(AMBOS, K. 2006:153)⁵⁶⁶ *Su presupuesto no podría ser que se haya actuado de acuerdo a derecho en el entorno del autor, pues de lo contrario se exoneraría de responsabilidad penal justamente a los autores de macrocrímenes. De hecho, la macrocriminalidad habría sido "atribuida" en la praxis judicial, habiéndose arribado en un número no pequeño de casos a una sanción y criminalización* (AMBOS, K. 2006:154)⁵⁶⁷.

Vemos ahora que según todo lo expuesto, en palabras de Ambos, que Jäger establece el objetivo del derecho penal internacional como *inter alia*, "*identificar y hacer visible la responsabilidad individual*".(AMBOS, K. 2006:154)⁵⁶⁸ *Sin embargo, como parte del derecho criminal, el derecho penal internacional serviría además a "la solución de conflictos" y, para ello, la pena no sería siempre el medio adecuado.* (AMBOS, K. 2006:154)⁵⁶⁹

El más reciente resultado doctrinal elaborado por Jager⁵⁷⁰ reitera nuevamente su opinión de que —a pesar de los problemas mencionados— *también en los macrocrímenes (políticos) el individuo podría ser el destinatario de la imputación de las normas jurídico-penales.* (AMBOS, K. 2006:154)⁵⁷¹ En este caso, el autor se ocupa ahora con más profundidad del "*derecho penal del sistema*" (AMBOS, K. 2006:154)⁵⁷² elaborado por Lampe, no viendo allí ninguna solución de los problemas esenciales de imputación. (AMBOS, K.

⁵⁶⁶ Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 153.

⁵⁶⁷ Ídem, p. 337 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁶⁸ Ídem, p. 348. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁶⁹ Ídem, p. 349 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷⁰ Jager, en: Lüderssen (editor), Kriminalpolitik III (1998), p. 122 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷¹ Ídem, p. 125, 129. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷² Lampe, ZStW 1994, 683 ss. (al respecto, para mayores detalles infra). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

2006:154)⁵⁷³ *Jager insiste en que sólo el derecho penal clásico individual podría hacer visibles los macroacontecimientos destructivos* (AMBOS, K. 2006:154)⁵⁷⁴ *y, por tal razón, sería preferible a una mera responsabilidad colectiva.*

5.1.4. Jakobs: exoneración del autor, responsabilización de los hombres de atrás o del sistema.

En este momento investigativo, es necesario analizar la postura de *Jakobs*, quien plantea como tesis la exoneración del autor y la responsabilización del “hombre de atrás”, es decir, el determinador, dándole esta calidad también al sistema. *Jakobs*, en palabras de Ambos, *analiza el problema de la repercusión de determinados diagnósticos psíquicos (costumbre, defectos de socialización y vínculos de la dinámica de grupos) sobre la culpabilidad bajo la óptica de la relación entre "hecho psíquico y norma".* (AMBOS, K. 2006:154)⁵⁷⁵ *Este autor parte de un concepto funcional de culpabilidad,* (AMBOS, K. 2006:154)⁵⁷⁶ *que coloca el concepto de capacidad (para la comprensión del injusto) en un "contexto funcional". La capacidad ("Fähigkeit") tendría que ser concebida, no en el sentido psicológico de "poder" ("Können"), sino normativamente como "competencia" ("Zuständigkeit"). Se debería construir un "equilibrio" entre el "individuo afectado psíquicamente" y la "sociedad necesitada de normas garantizadas". La afectación individual*

⁵⁷³ *Jager*, en: Lüderssen (editor), *Kriminalpolitik III* (1998), p. 130 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷⁴ Nuevamente *idem*, p. 137 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷⁵ *Jakobs*, en: Göppinger/Bresser (editores), *Sozialtherapie* (1982), p. 127 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

⁵⁷⁶ Cfr. ya supra § 1 III. 5. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

del autor sería sólo "un lado de la estructura a equilibrar"; del otro lado debería ser garantizada la "vigencia de las normas". Por ello, la exoneración individual de culpabilidad debería ser en todo caso "socialmente aceptable". Sólo bajo esta condición podría resolverse el conflicto en cuestión "de un modo diferente que el de la imputación del autor". (AMBOS, K. 2006:154)⁵⁷⁷

Esta concepción elaborada por Jakobs en 1982 es bastante reveladora, toda vez que deja de lado su postura de encausar la política criminal de los estados bajo la doctrina del Derecho Penal del Enemigo, y pasa a desarrollar una nueva postura en la que considera que la Culpabilidad, como elemento de la triada finalista (Tipicidad, antijuridicidad y culpabilidad), debe contar con un nuevo subelemento por así decirlo, en donde el sujeto no solo debe “poder” oponerse a la comisión de la conducta punible, sino que debe contar con un elemento psicológico, es decir, no estar afectado psicológicamente bajo ninguna circunstancia, así esta constituya a la normatividad en sí misma, pues el equilibrio entre el Estado y el sujeto es lo que permite configurar una verdadera adecuación típica antijurídica y culpable en cada caso.

Es primordial tener en cuenta las opiniones de Jakobs, en lo que en palabras de Ambos se refiere a lo concerniente *a las repercusiones de los diagnósticos psíquicos mencionados sobre la culpabilidad, aquí son de interés las reflexiones de Jakobs sobre los defectos de socialización y los vínculos de la dinámica de grupos. En el primer supuesto, Jakobs se refiere a modo de ejemplo a la sentencia del BGH en el caso Stachynski, en la cual, como es sabido, el autor directo (agente S.) fue caracterizado solamente como*

⁵⁷⁷ Jakobs, en: Göppinger/Bresser (editores), Sozialtherapie (1982), p. 128 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 154.

cómplice y los hombres de atrás (de la KGB) como autores principales. (AMBOS, K. 2006:155)⁵⁷⁸ Jakobs ve en ello "una aplicación del § 21 del StGB transpuesta a las categorías dogmáticas de la doctrina de la intervención" al hecho en favor del autor directo. (AMBOS, K. 2006:155)⁵⁷⁹ Su exoneración tendría lugar "exactamente a cambio de una responsabilización reforzada de los hombres de atrás" (AMBOS, K. 2006:155).⁵⁸⁰ Por tanto, no se renuncia a la resolución del conflicto a través de la imputación, sino que sólo se la desplaza a un nivel más alto. Se puede hablar de una imputación compensatoria a cuenta de los hombres de atrás. Para Jakobs se reconoce con ello el "defecto como diagnóstico psicológico, sin debilitar la garantía de la norma". (AMBOS, K. 2006:154)⁵⁸¹ Sólo por ello sería admisible la atenuación fáctica de la culpabilidad de Stachynski. La causalidad de un diagnóstico psicológico no diría per se nada sobre la culpabilidad o falta de culpabilidad; una causa exoneraría sólo en caso de que el autor no sea "competente" por ella. Esto puede ocurrir solamente si existe otro camino para la elaboración de la causa, por ejemplo, como en el caso Stachinsky, mediante la "responsabilización de otro sistema en lugar del autor".(AMBOS, K. 2006:155)⁵⁸² De este modo, también sería posible en principio atribuir los hechos en un sistema injusto al mismo sistema y eliminar al respecto la competencia del autor. Ciertamente, esto presupondría una distancia respecto

⁵⁷⁸ BGHSt 18, 87 ss.; Jakobs, en: Göppinger/Bresser (editores), Sozialtherapie (1982), p. 133 ss. N.deiT. El § 21 StGB regula la facultad de atenuación de pena para los casos de capacidad de culpabili-

dad disminuida (*verminderte Schuldhaftigkeit*). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

⁵⁷⁹ ídem, p. 133. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155

⁵⁸⁰ ídem, p. 134 (resaltado en el original). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

⁵⁸¹ ídem, p. 134. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

⁵⁸² ídem, p. 135. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

del régimen ilícito en cuestión, que posibilite "separar en el sistema las fuerzas de ese sistema de los titulares [...] del dominio".(AMBOS, K. 2006:155)⁵⁸³

Otra de las grandes y reveladoras ideas del creador de la Doctrina del Derecho Penal del Enemigo, gira en torno, en palabras de Ambos, a *la cuestión relativa a la medida en que los vínculos de la dinámica de grupos pueden repercutir sobre el juicio de culpabilidad.* (AMBOS, K. 2006:155)⁵⁸⁴ *La cuestión decisiva sería la de a quién se podría atribuir el riesgo de un "accidente de dinámica de grupos" (Schumacher): a la sociedad o a los miembros del grupo. Al respecto, para la resolución del conflicto quedaría sólo la imputación de los miembros individuales del grupo. Éstos seguirían siendo "competentes" —a pesar de las afectaciones (psíquicas) individuales— por su propia situación de coacción.*

Para solucionar cualquier problema, bajo la teoría de *Jakobs*, debemos ocuparnos, por recomendación de Ambos en determinar a *quién se puede solucionar un conflicto determinado. La respuesta dependería de la resolución de la cuestión de quién es "competente" por el conflicto y, por tanto, según criterios normativos y no meramente psicológicos: "Para una supresión o atenuación de la culpabilidad el autor debe poder ser distanciado del impulso [al hecho]; él no tiene que ser competente por el impulso".(AMBOS, K. 2006:156)⁵⁸⁵ En una prosecución consecuente de este punto de vista, también con relación a los hechos ilícitos de la DDR *Jakobs* ha reducido mencionadamente la responsabilidad individual de los autores —como "vainas personales rellenas con la sangre del sistema respectivo" (AMBOS, K.*

⁵⁸³ ídem, p. 135 s Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

⁵⁸⁴ ídem, p. 136 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 155.

⁵⁸⁵ ídem, p. 137. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

2006:156)⁵⁸⁶—, *resolviendo el conflicto a costa del sistema político, de la "política miserable"*(AMBOS, K. 2006:156).⁵⁸⁷ Con esto, él sólo ha aprovechado sus argumentaciones vertidas con anterioridad. (AMBOS, K. 2006:156)⁵⁸⁸

5.1.5. Lampe: derecho penal del sistema como complemento de la responsabilidad individual.

En este estadio investigativo es necesario tener en cuenta la postura de Lampe, autor reconocido y citado por Ambos dentro de su teoría de derecho penal internacional general, Lampe plantea la teoría de que el Derecho Penal del Sistema es un complemento de la responsabilidad individual.

Es así como Lampe, en palabras de Ambos, *intenta desarrollar una teoría del injusto de sistema y de la responsabilidad dentro de sistemas injustos, porque las categorías fundamentales de la dogmática penal que se utilizaron hasta ahora estarían hechas solamente a la medida del autor individual y serían demasiado "simples" para comprender adecuadamente el injusto de los sistemas injustos.* (AMBOS, K. 2006:156)⁵⁸⁹ Para Lampe, *la "dogmática de las acciones injustas" necesitaría, por consiguiente, un complemento mediante la "dogmática de los sistemas injustos"* (AMBOS, K. 2006:156)⁵⁹⁰ Para el autor

⁵⁸⁶ Jakobs, en: Isensee (editor), *Vergangenheitsbewältigung* (1992), p. 42. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁸⁷ *idem*, p. 56. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁸⁸ Cfr. *supra*, nota 92 y en el texto. Cfr. también ya *supra* § 1 III. 5. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁸⁹ Lampe, *ZStW* 1994, 683, 685 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁹⁰ *idem*, 687. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

en cita, con este término se habrían de entender las "relaciones de personas organizadas hacia objetivos ilícitos", a saber, sistemas criminales simples (grupos pequeños, especialmente la coautoría) y sistemas criminales constituidos (asociaciones criminales, empresas comerciales y el Estado). (AMBOS, K. 2006:156)⁵⁹¹

Es entonces teniendo en cuenta la definición de Lampe de dogmática de los sistemas injustos, que Ambos la define para su contexto del Derecho Penal General Internacional y frente a la imputación de conductas macrocriminales, así:

"En nuestro contexto se trata del caso mencionado en último término. A saber, de "formas estatales o Estados criminalmente pervertidos", es decir, Estados o instituciones estatales cuyos "funcionarios cometen delitos que son la expresión de la filosofía del Estado o que son provocados o favorecidos por medio de una falta consciente de controles jurídicos".(AMBOS, K. 2006:156)⁵⁹² Aquí no se trataría, por otra parte, del injusto del propio sistema, (AMBOS, K. 2006:156)⁵⁹³ sino de la responsabilidad penal dentro del sistema. (AMBOS, K. 2006:156)⁵⁹⁴ En este sentido Lampe se remite solamente a la teoría de Roxin del dominio por organización, (AMBOS, K. 2006:157)⁵⁹⁵ dedicándose luego —otra vez— a la responsabilidad penal del sistema injusto como tal. (AMBOS, K. 2006:157)⁵⁹⁶ Así, su verdadero objetivo es la

⁵⁹¹ Ídem, 688 ss., 693 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁹² Cfr. ídem, 700 ss. (702). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁹³ Cfr. ídem, 702 ss. (713 ss.). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁹⁴ Ídem, 716 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 156.

⁵⁹⁵ Ídem, 721 s., 743. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁵⁹⁶ Ídem, 722 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

responsabilidad colectiva; pero ésta no debe desplazar, por lo visto, la responsabilidad individual de un miembro de un sistema injusto, sino sólo completarla. En todo caso, Lampe reconoce la "autorresponsabilidad" de los miembros de una asociación criminal. (AMBOS, K. 2006:157)⁵⁹⁷ En cuanto concierne a los Estados, aunque Lampe considera dominante el punto de vista que afirma la responsabilidad penal individual, no lo comparte, ya que en su opinión sería "injusto": "pues una pena que sólo alcanza a personas no expía el injusto del sistema que provocó los crímenes y que, para ello, se procuró de asistentes".(AMBOS, K. 2006:157)⁵⁹⁸ En su opinión, se correspondería, más bien, con la idea de justicia que la pena se dirigiese en primera línea contra el sistema y en ello no se perjudicaría la justicia si ante todo fuera alcanzada la población. (AMBOS, K. 2006:157)⁵⁹⁹ Por otra parte, la mayor cantidad posible de inocentes deberían ser exceptuados de la "responsabilidad de consecuencia".(AMBOS, K. 2006:157)⁶⁰⁰ Si bien existirían reparos, especialmente de índole práctica, en contra de tal responsabilidad colectiva, éstos serían para Lampe "de poca importancia" (AMBOS, K. 2006:157)⁶⁰¹ en vista de la injusticia y los problemas de la persecución penal individual. Así, sería "casi ilusorio" comprender en términos probatorios el injusto individual "dentro de la red de la criminalidad organizada por el Estado".(AMBOS, K. 2006:157)⁶⁰² De todos modos,

⁵⁹⁷ ídem, 726 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁵⁹⁸ ídem, 735 ss. (738). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁵⁹⁹ ídem, 739. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁶⁰⁰ ídem, 740. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁶⁰¹ ídem, 740 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁶⁰² Sobre la problemática de la prueba en los procesos de Núremberg cfr. por ejemplo *Dodd*, JCLC&PS 1946/47, 357 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

existiría también una "responsabilidad de los funcionarios" del sistema desde un doble punto de vista: "por el injusto de sistema, al cual ellos tomaron parte en virtud de su posición en el aparato de poder, y por su propio injusto personal de acción".(AMBOS, K. 2006:157)⁶⁰³ En el primer caso, los miembros de un sistema injusto serían responsables por los crímenes de éste "cuando ellos, debido a su posición de dirigencia, eran competentes por la organización de los crímenes o por su preparación ideológica".(AMBOS, K. 2006:157)⁶⁰⁴

5.1.6. Naucke: Creación y desarrollo de una “cuarta vía de derecho penal”.

Naucke ha desarrollado la teoría de la cuarta vía del derecho penal, dentro de esta teoría, podemos considerar la primera vía como el *puro derecho penal en un Estado de Derecho*, la segunda vía y tercera vía como *las medidas de seguridad y corrección y el principio de reparación en lugar de pena* y la nueva denominada cuarta vía cuyo propósito es sancionar la criminalidad que ha sido reforzada o permitida por el Estado o en las cuales la estructura estatal como sistema ha participado.

La apreciación de Ambos sobre la doctrina elaborada por Naucke, se ha establecido en la pluricitada obra, así:

“En su ya citada monografía sobre la "criminalidad reforzada por el Estado", Naucke ha proclamado el desarrollo de una cuarta vía de derecho penal, destinada a combatir efectivamente este tipo de

⁶⁰³ *Lampe*, ZStW 1994, 741 ss. (742 s.). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

⁶⁰⁴ *ídem*, 745. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 157.

criminalidad. (AMBOS, K., 2006 P. 158)⁶⁰⁵ La primera vía (el puro derecho penal de un Estado de derecho (AMBOS, K., 2006 P. 158)⁶⁰⁶) sería, en su opinión —a causa de su conocida sujeción al derecho positivo y del límite de la prohibición de retroactividad—, demasiado limitada para esta misión.¹¹⁶ Las experiencias con la segunda y tercera vía (las medidas de seguridad y corrección y el principio de "reparación en lugar de pena") (AMBOS, K., 2006 P. 158)⁶⁰⁷ sugerirían "demarcar una zona del derecho penal" separada para la lucha contra la criminalidad reforzada por el Estado. (AMBOS, K., 2006 P. 158)⁶⁰⁸

Para Ambos, los contornos de esta cuarta vía vendrían trazados por el derecho penal internacional, aunque también podrían ser construidos en los derechos nacionales. Solamente se deberían utilizar con decisión las posibilidades jurídico-penales del positivismo, por ejemplo, concentrándose en los delitos graves, reconociendo la "incompetencia" de mecanismos (fácticos) de exención de la punibilidad tales como la prohibición de retroactividad, la prohibición de analogía y la fórmula del princeps legibus solutus. (AMBOS, K., 2006 P. 158)⁶⁰⁹

A modo de conclusión del pensamiento de Naucke, definido por Kai Ambos, frente a la cuarta vía, que permite la imputación de conductas macrocriminales

⁶⁰⁵ Naucke, Privilegierung (1996), p. 65 ss. (76 ss.). Cfr. también Naucke, FS Bemmman (1997), p. 75 ss., donde reclama nuevamente complementar el derecho penal "normal", protector del Estado, con un derecho penal "que proteja frente al Estado" (p. 81). Y continúa: un "derecho penal estrictamente conforme a un Estado de derecho" no excluiría el castigo de la criminalidad de Estado, sino que éste sería "su objeto principal" (p. 84). En esencia, prob. Hassemer, FS BGH IV (2000), p. 443 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶⁰⁶ Naucke, Privilegierung (1996), p. 73 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶⁰⁷ ídem, p. 76. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶⁰⁸ ídem, p. 74 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶⁰⁹ ídem, p. 76. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

donde se ha visto involucrado el Estado, ya sea por su permisividad, omisión o participación directa, tenemos:

"Se trataría, con esta vía, de una "forma de pensamiento" que existía también a la época de comisión de los hechos, sólo que no podía imponerse fácticamente. Ella habría querido ser utilizada ya mientras "reinaba]" el dictador y sería "la prueba que pone al descubierto que existe un tercer poder en el Estado". En fin, en ella estaría contenido — en consonancia con el art. 7, CEDH y el art. 15 (2), PIDCP (AMBOS, K., 2006 P. 158)⁶¹⁰— el derecho a sancionar la criminalidad reforzada por el Estado, que no pudo ocurrir en el momento del hecho únicamente por motivos fácticos. (AMBOS, K., 2006 P. 158)⁶¹¹ Aunque Naucke considera de peso las críticas contra esta nueva vía fundadas en los postulados de un Estado de derecho, en definitiva —en vista de la realidad político-criminal— no las considera decisivas. (AMBOS, K., 2006 P. 158)⁶¹² Primeramente —sostiene—, las otras vías del derecho penal deberían "ser reconducidas nuevamente a un derecho penal unificado de reacción a la criminalidad general y rigurosamente ligado a los postulados de un Estado de derecho". (AMBOS, K., 2006 P. 158)⁶¹³ La nueva cuarta vía se convertiría, así, en la segunda vía que, a largo plazo, también podría "ser reconducida en el derecho penal común": "De este modo, el debate sobre la falta de calidad, en términos de exigencias de un Estado de derecho, de una cuarta vía del derecho penal podría ser el comienzo de la nueva construcción de un derecho

⁶¹⁰ ídem, p. 76 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶¹¹ Cfr. ya supra § 1 I. 3. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶¹² Naucke, Privilegierung (1996), p. 77 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶¹³ ídem, p. 79 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

penal unificado y rigurosamente ligado a los postulados de un Estado de derecho". (AMBOS, K., 2006 P. 158)⁶¹⁴

5.1.7. Marxen: puntos de partida para una teoría del delito de derecho penal internacional.

Dentro de los autores catalogados como principales para Kai Ambos en el desarrollo investigativo de la imputación de conductas macrocriminales, es indispensable hablar de Marxen, quien consideramos realiza el aporte más importante para esta investigación denominada *EL DELITO EN LA CIBERSOCIEDAD Y LA JUSTICIA PENAL INTERNACIONAL*, pues es Marxen quien plantea las bases para crear una teoría del delito particular para juzgar las conductas enmarcadas dentro del derecho penal internacional, que es exactamente la propuesta que se desarrollará más adelante en este capítulo.

En palabras de Ambos, *Marxen ha invitado a la dogmática penal alemana a desarrollar una teoría del delito de derecho penal internacional. (AMBOS, K., 2006 P. 159)⁶¹⁵ Entiende por ella "un sistema de principios axiomáticos reconocidos para la comprensión conceptual del delito de derecho internacional".(AMBOS, K., 2006 P. 159)⁶¹⁶ Partiendo de la pretensión de "validez general" de la teoría alemana del derecho penal, se tendría que verificar "si la teoría general del delito podría reclamar ilimitada vigencia fáctica también en el terreno del derecho penal internacional" o si, por el contrario, sus particularidades exigirían una "teoría del delito" especial "de derecho*

⁶¹⁴ ídem, p. 80 (resaltado por el autor). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 158.

⁶¹⁵ *Marxen*, en: Lüderssen (editor), *Kriminalpolitik III* (1998), p. 220 ss. (220, 236). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

⁶¹⁶ ídem, p. 220. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

penal internacional".(AMBOS, K., 2006 P. 159)⁶¹⁷ En este sentido, habría que enfrentarse con un "problema de gravedad" y un "problema de estructura". El problema de gravedad consistiría en que sólo las conductas típicas de una determinada gravedad podrían representar un crimen de derecho penal internacional. (AMBOS, K., 2006 P. 159)⁶¹⁸ Para una determinación más precisa sería necesario un concepto material de delito, el cual, según Marxen, no proporcionaría la doctrina nacional.

El problema de estructura se relacionaría con la estructura de la imputación y de los tipos penales de derecho penal internacional. (AMBOS, K., 2006 P. 159)⁶¹⁹ Para Marxen, del Estatuto del ICTY resultaría que sólo están comprendidos aquellos hechos que han sido cometidos "sistemáticamente", es decir, en un contexto de organización, y que, a la vez, son "específicos del sistema", esto es, que están relacionados con un sistema político determinado. (AMBOS, K., 2006 P. 159)⁶²⁰ El problema de estructura consistiría, por tanto, en que la estructura tradicional del concepto de delito se orienta a la conducta individual y, por tal motivo, no sería apropiada para comprender la intervención al injusto sistemático. (AMBOS, K., 2006 P. 159)

Ahora veremos los principales planteamientos de la teoría de Marxen sobre la teoría del delito dentro del Derecho penal internacional, *Marxen toma de la sentencia de los juristas, sugeriría un "sistema de imputación" compuesto de "tres elementos y dos eslabones de comunicación":(AMBOS, K., 2006 P. 159)⁶²¹ El desarrollo esta nueva teoría del delito parta del primer elemento que estaría constituido por la "conducta concreta" de una persona determinada.*

⁶¹⁷ ídem, p. 223. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

⁶¹⁸ ídem, p. 223-6. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

⁶¹⁹ ídem, p. 226-36. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

⁶²⁰ ídem, p. 228. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

⁶²¹ ídem, p. 231 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 159.

Como segundo elemento aparecería el "contexto criminal supraindividual", por ejemplo, el programa criminal. Y finalmente, El tercer elemento consistiría en el resultado del crimen, por ejemplo, el homicidio de determinadas personas. Los dos eslabones de comunicación establecerían la relación de imputación entre estos elementos: un individuo intervendría en el proyecto criminal total y lo conduciría al resultado del crimen.

Entonces desde esta perspectiva de adecuación típica, antijurídica y culpable, la consecuencia —según Marxen—, al individuo sería imputada *"la intervención en un proyecto criminal total, el cual ha originado el resultado del crimen"*. (AMBOS, K., 2006 P. 160)⁶²² Comparada con la estructura tradicional de la imputación, esta imputación sería *"móvil"* *"por la inserción del elemento intermedio del proyecto total"*; entre la persona individual que actúa y el resultado del crimen no debería existir *"ninguna comunicación directa"*. (AMBOS, K., 2006 P. 160)⁶²³ Aunque esto recuerde la *"idea de la conspiracy"*, (AMBOS, K., 2006 P. 160)⁶²⁴ existiría una diferencia desde un doble punto de vista: La imputación de derecho penal internacional presupondría que se produzca un resultado del crimen y que el individuo lo conozca. Un análisis minucioso de este problema de estructura, así continúa Marxen, conduciría a descubrir paralelos entre la dogmática nacional y aquella de derecho penal internacional. Estos paralelos ya se han dejado ver en las soluciones propuestas por la dogmática nacional en relación con la intervención en el injusto colectivo, especialmente en el injusto de sistema, por ejemplo, en la teoría del dominio por organización. (AMBOS, K., 2006 P. 160)⁶²⁵

⁶²² Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

⁶²³ Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

⁶²⁴ Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

⁶²⁵ Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

5.1.8. Resumen valorativo.

Kai Ambos, a modo de conclusión frente a los planteamientos de los autores que generaron grandes aportes a la teoría de imputación de conductas macrocriminales logra establecer:

- a. *En primer lugar, es generalmente reconocido que también los hechos colectivos se componen de partes individuales distinguibles. Esto ya fue constatado por Peters y luego demostrado con más detalles por Jáger. Este autor habla convincentemente de la "dimensión individual" y "personal" del injusto colectivo (1968/ 69, 1980, 1985/ 89), de la "conducta coordinada del individuo" (1988), de la "re-transformación [...] en una persona" (1993) —siguiendo aquí a Hannah Arendt— o simplemente de la "responsabilidad individual" que debería hacerse visible (1995, 1998). También la criminología general (AMBOS, K., 2006 P. 160)⁶²⁶ y los otros autores aquí mencionados reconocen la dimensión individual del injusto colectivo. (AMBOS, K., 2006 P. 160)⁶²⁷ Si bien Lampe —el único— considera casi "ilusoria" la demostración del injusto individual, él es refutado por las sentencias de derecho penal internacional analizadas en ese trabajo. (AMBOS, K., 2006 P. 160)*
- b. *El segundo reconocimiento, que asimismo se atribuye a Jager (1985/89), es que los efectos de la dinámica de grupos y de los procesos de psicología de masas no tienen en el marco del injusto colectivo ninguna otra repercusión sobre el reproche jurídico-penal de*

⁶²⁶ Cfr. *Kaiser*, *Kriminologie* (1996), p. 432, en donde se expresa que también los sistemas se compondrían con el actuar del individuo. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

⁶²⁷ Cfr. también *Werle*, *ZStW* 1997, 822 s., quien resalta el efecto pacificador de los procesos penales internacionales, en los cuales se reconoce el pasado injusto y se individualiza la culpa. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 160.

culpabilidad que la mera atenuación de la culpabilidad. En conclusión, se puede constatar que la imputabilidad individual depende, en definitiva, de la medida en que en las acciones colectivas se puedan reconocer "efectos y rastros de tendencias, motivos e impulsos individuales", dando un paso atrás, por tanto, los modelos de acción "ajenos de personalidad" inmanentes a la comisión colectiva del hecho. (AMBOS, K., 2006 P. 161)⁶²⁸ También el concepto funcionalista de culpabilidad de Jakobs conduce sólo en casos de excepción a una exoneración del individuo, a saber, sólo cuando el conflicto originado por la comisión de un delito puede ser solucionado a costa del colectivo o del sistema injusto. Más arriba he designado esto como "imputación compensatoria". Tal "concepto funcionalista de autor" es, sin embargo, poco convincente, pues exonera al individuo, incluso al hombre de atrás, de toda responsabilidad penal a costa de un "sistema", cuya noción es prácticamente inaferrable. Como correctamente ha expresado Jager, este sistema se basa en un "estereotipo del autor

⁶²⁸ Por lo demás, el concepto de culpabilidad de Jakobs tiene que ser rechazado ya por las consideraciones fundamentales mencionadas anteriormente.¹⁴² En nuestro contexto, resulta de interés la crítica de Jager a las reflexiones de Jakobs antes expuestas sobre la relación entre hecho psíquico y norma. Según la opinión de Jager, la regulación legal del § 20 del StGB "no deja espacio para una re-interpretación puramente normativa del [...] concepto de 'capacidad', el cual claramente se tiene que entender en sentido 'psicológico'".¹⁴³ Sustancialmente, la interpretación de Jakobs acabaría "en una repatriación de ese elemento de la capacidad de culpabilidad que trasciende al universo conceptual del derecho al ámbito exclusivo de disposición de la ciencia del derecho" y, con ello, "en un reparto de los intereses sociales e individuales que, de antemano, no dejaría ninguna chance al individuo con afectaciones (psíquicas)". Frente a la necesidad de garantizar la vigencia de la norma, el individuo quedaría relegado "completamente a un segundo plano", a menos que no se encontrara "un destinatario sustituto de la imputación". El derecho penal de culpabilidad se convertiría, con ello, en un mero "derecho penal de ficción". Las posibles consecuencias de determinados diagnósticos psíquicos en el ámbito de la macrocriminalidad se encontrarían "bloqueadas y recortadas de antemano con la alusión a la prioridad de la vigencia y de la afirmación de la norma". A pesar de esta crítica —fundamentalmente correcta— no puede pasarse por alto que la concepción *jakobsiana*, como recién se ha expuesto, puede conducir también a la *exoneración* del individuo y a la *responsabilización* del sistema. Aunque por las razones esgrimidas esto no sea convincente, sirve de todas maneras para refutar en cierto modo el reproche de Jager de que Jakobs no dejaría "de antemano ninguna chance" al individuo. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 161.

funcionalizado que actúa sin una motivación propia" y, de este modo, en una concepción que en su polarización no es sostenible empíricamente, ni deseable desde un punto de vista político criminal: "Pues ni 'sistemas', ni 'ruedecillas' o 'envoltorios personales' pueden seriamente ser responsables de algo".(AMBOS, K., 2006 P. 161)⁶²⁹ Aunque la crítica de Jager no se corresponde más, por su generalidad, con el estado actual de la discusión sobre la responsabilidad de sistemas o colectivos, (AMBOS, K., 2006 P. 161)⁶³⁰ ella es acertada, sin embargo, en cuanto a que el actuar en el sistema no puede ser, por sí solo, un motivo suficiente para una exculpación. De este modo, el concepto de autor funcional significa en última instancia un rechazo a un consecuente derecho penal de culpabilidad. También Lampe rechaza el, por él llamado, "concepto estatal del derecho" de Jakobs: la voluntad estatal que se pusiera en contra de principios del derecho elementales no podría reclamar vigencia normativa y, por tal motivo, no sería una condición suficiente ni necesaria para el derecho. (AMBOS, K., 2006 P. 161)⁶³¹

- c. El tercer reconocimiento concierne al intento de Lampe de desarrollar un "derecho penal del sistema". Ante todo, el modelo de la responsabilidad colectiva ligado a este sistema no sustituye a la responsabilidad individual, sino que sólo debe complementarla. (AMBOS, K., 2006 P. 162)⁶³² Las objeciones fácticas de Lampe en contra de la comprobación de la responsabilidad individual son*

⁶²⁹ Jager, Makrokriminalitat (1989), p. 181. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 161.

⁶³⁰ Jager, en: Hankel/Stuby (editores), Strafgerichte (1995), p. 333 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 161.

⁶³¹ Cfr. S/S-Cramer/Heine (2001), previamente a los § 25 ss., nrn. 130 con referencias. Lampe, ZStW 1994, 710. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 161.

⁶³² En favor de una responsabilidad *concurrente* de las personas jurídicas, también Heine, Verantwortlichkeit (1995), p. 269, 308. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

refutadas, como ya se ha dicho, por la praxis de derecho penal internacional. Este autor reconoce, además, la responsabilidad penal de los "funcionarios" de un sistema injusto desde un doble punto de vista: por su participación en el sistema injusto y por su injusto personal de acción. En cuanto concierne ahora al mismo modelo de Lampe, ha sido nuevamente Jager quien ha presentado las objeciones fundamentales en su contra. (AMBOS, K., 2006 P. 162)⁶³³ En mi opinión, este modelo parte ya de una premisa falsa, a saber, la de la culpa colectiva de un pueblo por los crímenes de la dirección de su Estado. Sólo quien comparte esta premisa puede sostener, como Lampe, que la justicia no se perjudicaría si se alcanzara "ante todo a la población". (AMBOS, K., 2006 P. 162)⁶³⁴ Una mera responsabilidad colectiva contradiría también, y justamente, uno de los objetivos principales de la utilización del derecho penal individual en contra del injusto colectivo, tal como ha sido formulado en el primer reconocimiento, a saber, el hacer visible los macrosucesos destructivos. (AMBOS, K., 2006 P. 162)⁶³⁵ Todos estos reparos no deben poner en duda, sin embargo, el sentido de las reflexiones sobre la adecuada consideración del lado colectivo del injusto de derecho penal internacional. (AMBOS, K., 2006 P. 162)⁶³⁶ Ellos pretenden solamente evidenciar que ninguno de estos caminos conduce directamente al desarrollo de reglas para la responsabilidad individual; de allí, que no se pone en discusión el desarrollo de reglas paralelas

⁶³³ Jager, en: Lüderssen (editor), *Kriminalpolitik III* (1998), p. 130 ss.; también *el mismo*, ya en: Hankel/Stuby (editores), *Strafgerichte* (1995), p. 330. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

⁶³⁴ Lampe, *ZStW* 1994, 739 Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

⁶³⁵ Cfr. también Jager, en: Lüderssen (editor), *Kriminalpolitik III* (1998), p. 137 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

⁶³⁶ Cfr. recientemente Vest, *ZStW* 2001, 489 ss., así como infra § 8 II. 4. c) dd). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

sobre la responsabilidad estatal o colectiva. (AMBOS, K., 2006 P. 162)⁶³⁷

- d. *De la praxis existente de derecho penal internacional Marxen ha desarrollado —en cierto modo como cuarto reconocimiento— una "relación de imputación [...] de tres elementos y dos eslabones de comunicación". De este modo, el pensamiento de Naucke de una "cuarta vía de derecho penal" experimenta un consecuente desarrollo y una necesaria concretización en cuanto a una teoría de la imputación de derecho penal internacional. La verdadera diferencia entre la concepción de Marxen y la imputación individual 'normal' consiste en que aquella considera como (segundo) elemento especial el "contexto criminal supraindividual" típico de la macrocriminalidad y flexibiliza la imputación "mediante la inserción del elemento intermedio del proyecto total". En el derecho penal internacional vigente esta concepción emerge con mayor claridad en la punición de la contribución "de algún otro modo" al hecho colectivo conforme al art. 25, tercer apartado, (d) del ECPI. (AMBOS, K., 2006 P. 1632)⁶³⁸ La concepción de Marxen se refiere, sin embargo, sólo al primer nivel de la imputación de derecho penal internacional, es decir, al nivel de la responsabilidad individual, sin considerar el de las defences. Desde el punto de vista metódico, es también cuestionable su limitación a la sentencia de los juristas como única fuente de derecho penal internacional. (AMBOS, K., 2006 P. 163)*

⁶³⁷ Cfr. también el art. 25 (4), ECPI, así como los trabajos de la ILC sobre la responsabilidad de los Estados (cfr. Crawford, EJIL 1999, 435 ss.). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 162.

⁶³⁸ Aquí, depende de las circunstancias del caso concreto si en primer lugar ha de efectuarse la imputación de una conducta determinada a un colectivo o a una persona natural (de otra opinión Schlösser, Verantwortlichkeit (2004), p. 31, 46 s., que quiere imputar primeramente al sistema). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 163.

De esta forma Kai Ambos logra resumir y así mismo considerar nuevas teorías que permiten, en casos como el planteado en la presente investigación Doctoral, lograr la imputación de conductas macrocriminales que se enmarcan dentro del Derecho Penal Internacional, logrando para los sujetos activos de la conducta (ya sean individuales o colectivos) una forma de adecuación jurídica a sus conductas que se adapte a los nuevos descubrimientos y avances sociales, y que al mismo tiempo tenga en cuenta a los Estados como sujetos activos de las conductas, de modo que no puedan endilgar la culpa a quien actúa, posiblemente, bajo una coacción psicológica y debe ser entonces, el Estado, como hombre de atrás quien asuma la responsabilidad penal por la comisión de cada conducta punible que logre establecerse.

Es así como puede concluir Ambos: *La especialidad de la imputación de derecho penal internacional consiste en que los hechos individuales —por lo general, codificados en los ordenamientos jurídico-penales nacionales— se insertan en un hecho total ("Gesamttat"), el cual describe el respectivo contexto colectivo de comisión. Este punto de vista completa la desde siempre conocida imputación individual (..), con un elemento colectivo, la imputación a la organización (criminal), por lo general, el Estado. Visto de este modo, se trata, por una parte, de un modelo de imputación no sólo individual, sino también "sistémico". (AMBOS, K., 2006 P. 163)⁶³⁹ Por otra parte, es posible hablar de una doble imputación, (AMBOS, K., 2006 P. 163)⁶⁴⁰ en el sentido de que la imputación individual y la colectiva/sistémica no se encuentran desvinculadas la una de la otra, sino que están en relación recíproca. (AMBOS, K., 2006 P. 163)⁶⁴¹ A diferencia del derecho penal nacional*

⁶³⁹ Cfr. sobre esto § 6 I, 2 y con más detalles infra § 8 III. 2 c). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 163.

⁶⁴⁰ Cfr. aparte de Marxen (supra 6), Vogel, ZStW 114 (2002), 409 s., 420 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 163.

⁶⁴¹ Schlösser, Verantwortlichkeit (2004), p. 30 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 163.

puramente individual, la existencia del hecho total en derecho penal internacional conduce a que en este ámbito se refiera siempre (también) a una organización o a un sistema. Considerando conjuntamente la imputación colectiva e individual, se plantea la pregunta, por un lado, acerca de la posición o bien función de los intervinientes en la organización en cuestión y, por el otro, sobre su contribución al hecho total de derecho penal internacional. Ambos puntos de vista —y no por ejemplo sólo la función de la persona en cuestión dentro de la organización— deciden sobre la clasificación jurídica de la intervención; tal modelo de imputación se dirige en primera línea contra los titulares de la decisión de la organización respectiva, dado que sólo ellos pueden dirigir con plena responsabilidad el hecho total. (AMBOS, K., 2006 P. 164)⁶⁴² Con esto resulta evidente que adquieren especial importancia los modelos de imputación normativizantes y fundados en la vigilancia, (AMBOS, K., 2006 P. 164)⁶⁴³ tales como se han desarrollado en la forma de la doctrina del dominio por organización y en la responsabilidad del superior. Por el contrario, la responsabilidad basada en la intervención en una "empresa criminal conjunta" ("joint criminal enterprise") desarrollada por la reciente jurisprudencia penal internacional se presenta como una imputación

⁶⁴² Cfr. Schlösser, *Verantwortlichkeit* (2004), p. 33 ss. (39: método de imputación funcional-social), así como p. 46 ss., donde él se dirige especialmente contra una concepto unilateral funcional-social de autor (49 ss.). En la práctica internacional esta tendencia se ha reforzado con la "completion strategy" de los Tribunales Ad Hoc (ICTY y ICTR). Así el Consejo de Seguridad de la ONU demandó del ICTY concentrar sus esfuerzos a los "most senior leaders suspected of being most responsible" para los crímenes dentro de su competencia (cfr. Declaración del Presidente del Consejo de Seguridad, UN Doc. S/PRST/2002/21, 23 de julio de 2002; Resol. 1505 (2003), 28 de agosto de 2003, UN Doc. S/RES/1503 (2003). Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 164.

⁶⁴³ Sobre un modelo de imputación "fundado en la vigilancia" ("supervisionistisch") y sobre otros (cinco) modelos de imputación cfr. Jung, en: Eser/Huber/Cornils (editores), 1998, 180 ss. (182 s.); profundizando Heine, en: Eser/Yamanaka (editores), 2001, 101. Sobre un modelo de imputación "normativizante" y sobre otros (once) modelos de imputación cfr. Vogel, ZStW 114 (2002), 406 ss., 419 s. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 164.

institucionalista-participatoria (AMBOS, K., 2006 P. 164)⁶⁴⁴ o *sistémica*. (AMBOS, K., 2006 P. 164)⁶⁴⁵

5.2. REPERCUSION DE LA SOCIEDAD DEL RIESGO EN EL ORDENAMIENTO JURÍDICO PENAL.

5.2.1. Derecho A La Seguridad:

En este aparte de la presente investigación debemos analizar lo concerniente al Derecho a la Seguridad dentro del Derecho penal del Riesgo. Castro, Henao, y Balmaceda, realizan este estudio donde establecen que *el antecedente que parece tener una significación concluyente en el nacimiento del Derecho Penal del riesgo es la mencionada sensación de inseguridad que hace brotar la demanda social de control esencialmente penal a la que el Estado, por diversos motivos, no es indolente ni le da siempre la solución más lógica* (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁴⁶. *Por ello, la apreciación política que cada una de las prevenciones político criminales novedosas debe conseguir, depende de cuando se pondera la libertad frente a la intromisión estatal* (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁴⁷. Frente a la determinación de cómo se configura el “Riesgo” en una sociedad, los autores en cita establecen que *de la forma en que se esboza la discusión*

⁶⁴⁴ Cfr. Jung, en: Eser/Huber/Cornils (editores), 1998, 183 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 164.

⁶⁴⁵ Vogel, ZStW 114 (2002), 420 ss. Citado en AMBOS, K. 2006. La parte general del Derecho Penal Internacional. Bogotá D.C.: Ed. Temis. Pag. 164.

⁶⁴⁶ Cfr. Mendoza Buergo, Blanca: El Derecho Penal ..., op. Cit., pp. 34 y ss; la misma: “Gestión del riesgo”, op. Cit., pp. 71 y ss. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 49

⁶⁴⁷ Cfr. Paredes Castañón, José Manuel: “Sobre el concepto”... op. Cit., p. 117. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 49

sobre la variación que experimenta el Derecho Penal frente a la sociedad del riesgo, el primer asunto digno de discusión que nace es el de delimitar hasta dónde los supuestos nuevos peligros son realmente nuevos. (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁴⁸ Entonces, la circunstancia terminante a recalcar es que en este nuevo entorno en el que nacen los nuevos peligros para bienes jurídico penales protegidos o protegibles (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁴⁹ van de la mano ciertos elementos que entorpecen gravemente la posibilidad de actuación del Derecho Penal, así como su efectividad, que pueden incluso llegar a perjudicar su legitimidad. Estos elementos pueden ser, a saber: (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁵⁰

- 1. La falta de capacidad de controlar cabalmente los efectos de la técnica.*
- 2. La explosión de ignorancia que va unida a la capacidad mencionada.*
- 3. En suma, el hecho de que el progreso normalmente se lleva a cabo por medio de organizaciones complicadas y jerarquizadas.*

Son los tres requisitos anteriores los que permiten crear el nuevo régimen de imputación en la sociedad del riesgo, estas peculiaridades hacen que el sistema de imputación y el régimen jurídico aplicable al sector riesgoso puedan ofrecer una respuesta, en pos de la eficacia, de modo imperioso a las

⁶⁴⁸ Como señala paredes Castañón, de lo que se trata es de esclarecer la especificidad que despliegan los riesgos para los bienes jurídicos-penalmente protegidos cuando ellos emanan de una acción humana tecnificada (Cfr. Su “Sobre el concepto...”, op. Cit., p. 119) Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 49

⁶⁴⁹ Cfr. Paredes Castañón, José Manuel: Riesgo y Política criminal: la selección de bienes jurídico-penalmente protegibles a través del concepto de riesgo sistémico. En AA.VV, la seguridad en la sociedad del riesgo..., op. Cit., pp. 93-94, y passim. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 49

⁶⁵⁰ Cfr. Mendoza Buergo, Blanca: El derecho penal..., op cit. Pp. 42 y ss. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 49

nuevas necesidades, la cual no siempre es legítima o verdaderamente eficaz. (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:50)⁶⁵¹

Para el caso Colombiano, los autores en cita desarrollan *en este contexto, y como no puede ser de otra forma* (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)⁶⁵², *las reformas legislativas implementadas en los últimos años en el ordenamiento punitivo se caracterizan por una relajación en el plano garantístico, como evidencian las siguientes notas:*

- *En primer término, la progresiva “espiritualización” del objeto de tutela, abudando en el Código los bienes de carácter colectivo o difuso, con perfiles insuficientemente definidos*
- *En estrecha conexión con la nota anterior, un increment notable de los delitos de peligro abstracto, cuyo riesgo radica, no tanto en el adelantamiento de la barrera de defense que comportan, como en la deficient técnica de tipificación del injusto que suele calificarlos*
- *En tercer lugar, el recurso creciente a los términos normativos y las constantes remisiones a otras disposiciones extrapenales, con vulneración de las exigencies dimanantes del principio de legalidad, y*
- *Finalmente, un aumento de los tipos omisivos, mediante los cuales se impone a los ciudadanos la obligación de realizar determinadas acciones, tendientes no solo a combatir los riesgos creados por el uso de las nuevas tecnologías, sino tambien al logro de la finalidad de homogenización económico-social asumida como propia por el Estado*

⁶⁵¹ Cfr. Mendoza Buergo, Blanca: “Gestión del Riesgo”, op. Cit., pp. 7-80. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 50

⁶⁵² Cfr. Mendoza Buergo, Blanca: El derecho penal..., op cit. Pp. 27-31. Citado en: CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez. P. 50

Intervencionista. Lo que explica que el ámbito de la omisión punible que no se haya ampliado unicamente en los campos del tráfico rodado, de la seguridad del trabajo, etc. sino tambien en material tributaria. (CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009:49)

Las reflexiones y consideraciones en la obra Derecho Penal en la sociedad del riesgo, fundamentan la persecución de los ciberdelitos por parte de la Justicia Penal internacional, justificando la nueva técnica de persecución por encima de la soberanía de los Estados y encontrando como nueva teoría para protección del riesgo y garantizar los derechos de las víctimas que su investigación, juzgamiento y condena se realice a través de la Corte Penal Internacional, teniendo como objetivo el establecimiento de una política criminal universal para los delitos informáticos donde el Derecho Penal no se utilizaría como límite sino como medio para efectivizarla.

Los impedimentos para efectivizar esta persecución penal, nacen de las dificultades sociales y legislativas que se relacionan directamente con la rapidez con la que evolucionan los medios para la comisión de los delitos y la lentitud de los sistemas jurídicos tradicionales para conocerlos, investigarlos, juzgarlos y condenarlos.

5.3. TEORÍA DE LOS CRÍMENES INTERNACIONALES

5.3.1. LOS CRÍMENES INTERNACIONALES COMO «CRÍMENES DE LESA HUMANIDAD»

Alejandro Chehtman, en su obra *Fundamentación filosófica de la justicia penal extraterritorial*, nos entrega las bases para establecer nuestra teoría según la cual un Tribunal Internacional y especializado debe encargarse de la

investigación, juzgamiento y sanción de los delitos informáticos. Así, Chehtman plantea que: *“Puede sostenerse que los argumentos más elaborados para dar cuenta de los rasgos centrales de los crímenes internacionales han sido desarrollados en el marco de lo que podríamos llamar el paradigma de los «crímenes de lesa humanidad»⁶⁵³. Este paradigma no necesariamente se concentra en la categoría jurídica de los crímenes de lesa humanidad, como algo distinto de los crímenes de guerra, el genocidio o los crímenes contra la paz (agresión). Más bien, se refiere usualmente a la visión tradicional, que posiblemente se remonte a la Cláusula de Martens incluida por primera vez en el Preámbulo del (II) Convenio de La Haya de 1899, según la cual los crímenes internacionales dañan o violan de alguna manera a la humanidad en sí misma⁶⁵⁴. Este daño a la humanidad supuestamente explicaría por qué un Estado extraterritorial o un tribunal internacional podrían tener derecho a castigar a los perpetradores de este tipo de crímenes. Es interesante destacar aquí que ha sido en el contexto de los crímenes de lesa humanidad como categoría jurídica (es decir, como algo distinto de los crímenes de guerra, el genocidio o los crímenes contra la paz) que los juristas y los tribunales han sido llamados a distinguir los delitos internos de los crímenes internacionales⁶⁵⁵. Los crímenes de guerra y los crímenes contra la paz, en cambio, ingresaron en la constelación de los crímenes internacionales*

⁶⁵³ Cfr. los escritos de Anupam CHANDER, «Globalization and Distrust», *Yale LJ*, 114 (2005); Adil Ahmed HAQUE, «Group Violence and Group Vengeance: Toward a Retributivist Theory of International Criminal Law», *Buffalo Crim L. Rev.*, 9 (2005); VERNON, «What Is Crime against Humanity?», 283; LUBAN, «A Theory of Crimes against Humanity»; MAY, *Crimes Against Humanity*. Me concentraré principalmente en los últimos dos. Citado en: CHEHTMAN, A. (2013:139). *Fundamentación filosófica de la justicia penal extraterritorial*. Madrid: Marcial Pons.

⁶⁵⁴ Preámbulo a la Convención de La Haya de 1899 (II). Véase, también, *Fiscal v. Erdemovic*, Caso núm. IT-96-22 [Sala de Primera Instancia, Fallo condenatorio (29 de noviembre de 1996)], §28. Citado en: CHEHTMAN, A. (2013:139). *Fundamentación filosófica de la justicia penal extraterritorial*. Madrid: Marcial Pons.

⁶⁵⁵ Phillis HWANG, «Defining Crimes against Humanity in the Rome Statute of the International Criminal Court», *Fordham International LJ*, 22 (1999); Beth VAN SCHAACK, «The Definition of Crimes against Humanity: Resolving the Incoherence», *Columbia J. of Transnational Law*, 37 (1999). Citado en: CHEHTMAN, A. (2013:139). *Fundamentación filosófica de la justicia penal extraterritorial*. Madrid: Marcial Pons.

con muy poca oposición. Tanto es así, que el primer criterio utilizado para «internacionalizar» los crímenes de lesa humanidad fue precisamente el «nexo con un conflicto armado»⁶⁵⁶. CHEHTMAN, A. (2013:139)

Con el planteamiento anterior, el autor en cita genera el primer punto de partida para crear competencia internacional en el ámbito penal, reduciéndola únicamente a ciertos delitos con características particulares, que según su desarrollo dogmático no podrían incluirse los delitos informáticos o ciberdelitos.

Aun así, los delitos definidos anteriormente han creado dentro del ámbito del derecho penal internacional una semejanza automática con la denominación de delito internacional, como lo explica Chehtman: *“En cualquier caso, actualmente los crímenes de lesa humanidad se han establecido como una categoría de crímenes internacionales por derecho propio y algunos hasta sostienen que podrían eventualmente volverse sinónimos de éstos⁶⁵⁷”*. CHEHTMAN, A. (2013:139)

No obstante lo anterior, este autor desglosa la teoría anterior en 3 puntos, que nos permiten adecuar desde la doctrina del derecho internacional, una justificación para el juzgamiento a través de un tribunal internacional los ciberdelitos, así lo establece Chehtman:

⁶⁵⁶ Véase, por ejemplo, M. Cherif BASSIOUNI, *Crimes Against Humanity in International Criminal Law* (2.^a ed., The Hague: Kluwer, 1999), 70-77, y Roger CLARK, «Crimes Against Humanity», en George GINSBURGS y V. N. KUDRIAVTSEV (eds.), *The Nuremberg Trials and International Law* (Londres: Martinus Nijhoff, 1990), 190-192. Citado en: CHEHTMAN, A. (2013:139). Fundamentación filosófica de la justicia penal extraterritorial. Madrid: Marcial Pons.

⁶⁵⁷ William J. FENRICK, «Should Crimes against Humanity Replace War Crimes?», *Columbia Journal of Transnational Law* 37 (1998-1999). Para la visión de que los crímenes de guerra son más apropiados como sinónimos de los crímenes internacionales, véase Gerry SIMPSON, *Law, War and Crime* (Londres: Polity Press, 2007). Citado en: CHEHTMAN, A. (2013:140). Fundamentación filosófica de la justicia penal extraterritorial. Marcial Pons: Madrid.

“Una primera línea general de argumentación se basa en la proposición de que los crímenes de lesa humanidad son crímenes internacionales porque son perpetrados por Estados u organizaciones similares a las estatales contra grupos bajo su control. Esto es, la consideración que los vuelve crímenes internacionales es el carácter grupal de sus perpetradores. Hay muchas versiones de este argumento. Para que la exposición sea lo más clara posible, podemos dividir las aquí en tres: a) la proposición analítica de que una autoridad extraterritorial tiene la facultad de castigar a un individuo por un crimen internacional sobre la base de que el Estado en el que el crimen fue cometido ha perdido (forfeited) su inmunidad ante ese tipo de intervenciones «extranjeras»; b) el argumento normativo que sostiene que la competencia penal de un Estado extraterritorial se basa en los intereses de las potenciales víctimas en el Estado en el que los crímenes fueron cometidos y en otros Estados afectados, y c) el argumento de que esta facultad debe ser explicada por referencia al interés individual de cada persona en la Tierra (esto es, los miembros de la especie humana). CHEHTMAN, A. (2013:141)

Centrémonos en la primera posición. Se ha sostenido que cuando las fuerzas de seguridad o los oficiales estatales del Estado E perpetran crímenes de lesa humanidad contra parte de la propia población de E, E carece de un derecho en contra de que otros «interfieran en sus asuntos internos», en particular, castigando a los perpetradores⁶⁵⁸. Esta proposición es intuitivamente plausible. ¿Por qué un Estado como ése retendría un derecho contra este tipo de interferencia? El problema, sin embargo, es que no se brinda una explicación explícita de por qué

⁶⁵⁸ LÜBAN, «A Theory of Crimes against Humanity», 109. Esto también es lo que Larry May llama el «principio de seguridad» (véase su *Crimes Against Humanity*, 63 -69). Citado en: CHEHTMAN, A. (2013:141). *Fundamentación filosófica de la justicia penal extraterritorial*. Marcial Pons: Madrid.

el Estado en el que el crimen fue cometido ha perdido su derecho prima facie en contra de que un determinado agente extraterritorial en particular castigue a los perpetradores. Justificar esta consecuencia normativa es más difícil de lo que puede parecer a simple vista. Ilustraré esta afirmación a través de un ejemplo interpersonal. Si A intenta matar a B disparándole con un revólver, A probablemente carezca de un derecho en contra de que terceras partes intervengan para salvar la vida de B (incluso matando a A si es necesario). Esto se explica frecuentemente por referencia al hecho de que A perdió su derecho en contra de ser atacado⁶⁵⁹. Sin embargo, una vez que la amenaza cesa, una tercera parte necesitaría otra justificación para usar la fuerza contra A (a nuestros efectos, para castigarla)⁶⁶⁰. CHEHTMAN, A. (2013:141)

Entonces si tomamos las tres premisas del autor *idém* para sustentar nuestro planteamiento, podemos justificar desde la doctrina el por qué los ciberdelitos deben ser investigados, juzgados y sancionados por un tribunal con competencia internacional. Chehtman sustenta su argumentación en estas tres aristas: a) *la proposición analítica de que una autoridad extraterritorial tiene la facultad de castigar a un individuo por un crimen internacional sobre la base de que el Estado en el que el crimen fue cometido ha perdido (forfeited) su inmunidad ante ese tipo de intervenciones «extranjeras»*; b) *el argumento normativo que sostiene que la competencia penal de un Estado extraterritorial se basa en los intereses de las potenciales víctimas en el Estado en el que los crímenes fueron cometidos y en otros Estados afectados*, y c) *el argumento de que esta facultad debe ser explicada por referencia al interés individual de cada persona en la Tierra (esto es, los miembros de la*

⁶⁵⁹ Véanse Judith Jarvis THOMSON, «Self-Defense», *Philosophy & Public Affairs* 20 (1991), 283- 310 y Suzanne UNIACKE, *Permissible Killing: The Self-Defence Justification of Homicide* (Cambridge: Cambridge University Press, 1994). Citado en: CHEHTMAN, A. (2013:141). Fundamentación filosófica de la justicia penal extraterritorial. Marcial Pons: Madrid.

⁶⁶⁰ Al respecto, véase el capítulo I. Citado en: CHEHTMAN, A. (2013:141). Fundamentación filosófica de la justicia penal extraterritorial. Marcial Pons: Madrid.

especie humana). Analizando la primera de ellas, es claro que cuando un delincuente informático ha sobrepasado las barreras que las naciones han implementado dentro de su política criminal para la protección de todos aquellos bienes jurídicos que pueden ser vulnerados a través de los medios informáticos, es porque dicho Estado no logra controlar de forma suficiente la comisión de estos delitos, y ha fallado en la protección al ser humano frente a estos ciberdelitos. El literal b, se refiere a los intereses del Estado en las víctimas de los delitos y la dificultad territorial que el mundo virtual genera para definir la competencia penal en este tipo de conductas, obliga a las naciones a remitir su conocimiento a un tribunal internacional y especializado que logre abarcar la protección a las víctimas independientemente de su localización geográfica, y finalmente, al analizar la tercera premisa, encontramos que esta misma protección referida en el literal b, solo busca reivindicar al hombre en su misma especie, es decir, luchar por la protección de su dignidad humana.

5.4. TRIBUNALES PENALES INTERNACIONALIZADOS: LA ESPECIALIZACIÓN DE LA JUSTICIA PENAL.

5.4.1. Introducción.

En este estadio de la investigación, ya habiendo determinado el modelo de imputación de conductas macrocriminales y conductas delictuales colectivas en el Derecho penal internacional, se hace necesario valorar la especialización de la Justicia Penal Internacional en el ámbito de los tribunales internacionales existentes, es por eso que citamos al autor español JUAN MANUEL RODRÍGUEZ BARRIGÓN, quien plantea que *La evolución más reciente del Derecho Internacional ha tenido una de sus expresiones más avanzadas en la profundización de los mecanismos de aplicación del Derecho Penal Internacional como fórmula jurídica de la lucha contra la impunidad. La*

multiplicación a partir del decenio de los 90 de los Tribunales penales internacionales, aun no siendo una novedad en la Sociedad Internacional Contemporánea, permite constatar la diversificación de medios y técnicas destinados a dotar de eficacia a la aplicación de las normas penales, pero también invita a subrayar la notable entidad que se otorgan a las mismos en nuestros días. (RODRÍGUEZ BARRIGÓN, J.M. 2006:331)⁶⁶¹

Para el autor en cita, *La constitución de estos Tribunales responde a finalidades específicas destinadas a dotar de efectividad a las normas internacionales penales que deben aplicar, pero debe tenerse presente que no constituye un fenómeno aislado si observamos la proliferación de órganos de naturaleza judicial que operan en el ámbito internacional, fruto de la diversificación y expansión del Derecho Internacional (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 331)⁶⁶². Ahora bien, circunscribiéndonos al objeto que en este estudio se aborda, conviene hacer notar la extensión y la pluralidad de modelos de justicia penal que se ha producido en el ámbito internacional, teniendo como impulso creador normas de diferente naturaleza y entidad que acomodan su aplicación en este sector especializado del orden jurídico internacional. Ciertamente, no puede dejar de subrayarse la importancia que las mismas tienen para la construcción del sistema jurídico internacional, cuyo análisis revela su impronta en diferentes terrenos del Derecho Internacional; no obstante, tampoco puede desconocerse que su adecuada comprensión debe conectarse con la inevitable sumisión a consideraciones de amplia envergadura en el campo de las relaciones*

⁶⁶¹ RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 331

⁶⁶² Evocamos de este modo los términos Internacionalesl empleados en el Informe del Grupo abril de 2006). **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 331

políticas (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)⁶⁶³. Este proceso de internacionalización de la justicia penal debe ser puesto en relación con el sobresaliente desarrollo que ha conocido el Derecho Internacional Penal en la última década del siglo XX. Ciertamente es que algunos de sus componentes fundamentales se habían ido fraguando en momentos históricos anteriores (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)⁶⁶⁴, pero debe reconocerse que estos avances relevantes se han producido en la definición progresiva de crímenes que son objeto de persecución en virtud de su tipificación mediante normas internacionales que son generalmente aceptadas, y con las que se protegen intereses fundamentales de la Comunidad Internacional. Como se ha destacado con frecuencia, esta evolución ha transformado de forma singular la posición del individuo en el orden jurídico internacional (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)⁶⁶⁵, y ha encontrado cauces procesales complejos en una última etapa hasta el momento con la creación del Tribunal Penal Internacional, que se impulsa bajo el principio de complementariedad de la jurisdicción internacional con las jurisdicciones de los Estados. (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)

⁶⁶³ Como puede observarse en el trabajo de J. MÉGRET: «The Politics of International Criminal Justice», *European Journal of International Law*, Vol. 13, núm. 5, 2002, pgs. 1261-1284. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson Civitas P. 332.

⁶⁶⁴ Para comprender esta evolución, puede verse el estudio de V. PELLA: «La co-dification du droit penal international», *Revue Générale de Droit International Public*, t. 56, 1952. Entre los documentos más avanzados en relación con la codificación de estos crímenes, puede verse el *Proyecto de Código de crímenes contra la paz y la seguridad de la Humanidad*, elaborado por la Comisión de Derecho Internacional en 1996 (*Informe de la Comisión de Derecho Internacional*, 48ª reunión, Doc. ONU A/CN.4/L. 522, 31 de mayo de 1996). **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson Civitas P. 332.

⁶⁶⁵ Sobre este particular, puede verse, entre otros, V. ABELLÁN HONRUBIA: «La responsabilité Internationale de l'individu», *Recueil des Cours de l'Académie de Droit International de La Haye*, Tome 280, 1999, pgs. 135-428. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson Civitas P. 332.

Tomando como base los fundamentos doctrinales anteriores se hace importante para el correcto desarrollo investigativo iniciar el análisis de cada uno de los tribunales internacionales, cuyo funcionamiento puede brindar bases para el modelo de justicia que pretendemos establecer.

5.4.2. La apertura de modelos de jurisdicciones penales internacionales: los tribunales *ad hoc*.

5.4.2.1. La internacionalización de la justicia penal.

Son los Tribunales Internacionales los que permiten que las conductas atentativas contra los bienes jurídicos tutelados dentro del Derecho Penal Internacional puedan ser investigadas, juzgadas y sancionadas, para el autor en cita, *El estudio de los tribunales penales internacionales tiene en nuestros días como punto de referencia fundamental la creación de los denominados tribunales ad hoc, cuyos perfiles quedaron definidos en 1993 con el Tribunal Penal Internacional para la ex Yugoslavia (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)⁶⁶⁶, y en 1994 con el Tribunal Penal para Ruanda⁶⁶⁷. Con ellos se instituyen tribunales internacionales en sentido estricto destinados a la aplicación de normas penales que se han venido consolidando en el orden internacional a partir de la Segunda Guerra Mundial. El objetivo de estos tribunales no era otro que impedir que cayeran en la impunidad los graves crímenes cometidos de forma sistemática en los conflictos que se desarrollaron en estos Estados. Es claro que estos tribunales internacionales nacen como una acción de carácter normativo frente a situaciones de grave*

⁶⁶⁶ Establecido por la Resolución 827 (1993) del Consejo de Seguridad de las Naciones Unidas, de 25 de mayo de 1993. Citado en: RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332

⁶⁶⁷ Cuyo establecimiento se previó en la Resolución 955 (1994) del Consejo de Seguridad de las Naciones Unidas, aprobada el 8 de noviembre de 1994." Citado en: RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332

violación de normas internacionales que hacen posible exigir responsabilidad penal a individuos, de manera que se estimó como una fórmula de reacción institucionalizada mediante la aplicación del Capítulo VII de la Carta. (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 332)

Para el autor en cita, la creación de los tribunales internacionales también puede definirse como una *respuesta hasta entonces desconocida en la práctica de Naciones Unidas, pero que ha tenido un notable impacto sobre la concepción de la responsabilidad penal del individuo en el Derecho Internacional. Como se sostiene de forma generalizada, las disposiciones de los Estatutos de estos Tribunales han recogido y sistematizado normas de Derecho Internacional Humanitario, cuya interpretación por las jurisdicciones que se crean facilitará la formación de un cuerpo interpretativo sobre el mismo.* (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 332).

Es entonces como se concluye que *la doctrina sentada por las decisiones de estos Tribunales ha cooperado eficazmente al desarrollo de este sector, con las limitaciones propias que se desprenden de su propia naturaleza* (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 332)⁶⁶⁸. Sin embargo son esas mismas limitaciones que contiene cada uno de estos Tribunales internacionales las que nos llevan al desarrollo de esta tesis, buscando un mecanismo que permita la investigación, juzgamiento y sanción de los cibercrímenes.

Frente a los tribunales existentes, es necesario resaltar los avances de su institucionalización, que en palabras de Fernández Liesa *Este proceso de institucionalización encuentra su punto álgido en 1998, cuando se concluye el*

⁶⁶⁸ Como anticipara A. PIGRAU I SOLÉ: noviembre de 1998, 12 de julio de 1999, 30 «La experiencia de los Tribunales penales internacionales para la antigua Yugoslavia y Ruanda», en *Hacia una justicia internacional*, Madrid, Ministerio de Justicia, 2000, pgs. 441-443. Citado en: RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 332

Estatuto de Roma de la Corte Penal Internacional RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 333)⁶⁶⁹, por el que se crea un tribunal permanente con competencia específica para la aplicación del Derecho Internacional Penal en los términos que establece el propio Estatuto, y en el que se comprenden los crímenes más graves que tienen una mayor trascendencia para la Comunidad Internacional. Como expresara CARRILLO SALCEDO, «nunca antes se había avanzado tanto en el camino de una justicia penal internacional digna de ese nombre» RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)⁶⁷⁰.

El principal logro de la creación y establecimiento del Estatuto de Roma es definido por el autor en cita así: *La entrada en vigor el 1 de julio de 2002 de este Tratado culmina una evolución de las jurisdiccionales penales internacionales que supera el carácter no permanente que tenían los Tribunales ad hoc constituidos en circunstancias específicas, pero además, tiene pretensiones globales, al posibilitar que quede sometido a él cualquier individuo acusado de graves violaciones de los Derechos Humanos y del Derecho Internacional Humanitario, con independencia del lugar donde éstos fueran cometidos. Ciertamente es que las aspiraciones de universalizar la jurisdicción de la Corte se encuentran ensombrecidas por el abierto rechazo que han expresado algunos Estados al mismo, o la ausencia de ratificación aún por un nutrido grupo de Estados que procedieron a su firma, pero ello no impide concluir su importancia capital en el proceso de afirmación del Derecho Internacional Penal.* RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332)

⁶⁶⁹ Contenido en el Documento A/ CONF. 183/9, de 17 de julio de 1998, enmendado por los procés-verbaux de 10 de noviembre de 1999, 12 de julio de 1999, 30 de noviembre, 8 de mayo de 2000, 17 de enero de 2001 y 16 de enero de 2002. Citado en: RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332

⁶⁷⁰ J. A. CARRILLO SALCEDO: «Presentación», en J. A. CARRILLO SALCEDO (coord.): *La criminalización de la barbarie: La Corte Penal Internacional*, Consejo General del Poder Judicial, Madrid, 2000, pg. 27. Citado en: RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 333

La permanencia establecida en el Estatuto de Roma, a través de la Corte Penal Internacional es la característica principal que debe contener un posible mecanismo de juzgamiento de los cibercrímenes, es claro que los avances sociales y tecnológicos no permiten crear una consideración de los delitos cibernéticos como temporales ni en el tiempo ni en el espacio, al contrario, se han convertido en conductas tan repetitivas en las sociedades que deben hacer parte de los tipos penales tradicionales por el aumento en su recurrencia.

Es entonces con la creación de la Corte Penal Internacional que según RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 332) *Surgen nuevas categorías de órganos cuya catalogación general puede ser incardinada entre los tribunales penales internacionales, con fórmulas ciertamente variables; pero en todo caso su comprensión debe ser puesta en relación con la diferenciación en sus grados de internacionalidad*⁶⁷¹.

5.4.2.2. La definición internacional de las jurisdicciones penales internacionales.

Viendo en capítulos anteriores la necesidad de la creación de un Tribunal internacional que permita la investigación, juzgamiento y sanción de los cibercrimes, debemos repasar teóricamente la definición de las jurisdicciones penales internacionales, donde encontramos el origen de estos cuerpos colegiados, que para casos como el de la Antigua Yugoslavia y Ruanda fueron

⁶⁷¹ R. KOLB: «Le degré d'internationalisation des tribunaux pénaux internationaux», en H. ASCENSIO, E. LAMBERT-ABDEL- GAWAD, J. M. SOREL (dirs.): *Les juridictions pénales internationalisées (Cambodge, Kosovo, Sierra Leone, Timor Leste)*, Société de Législation Comparée, París, 2006, pgs. 47-68. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson civitas P. 333.

creados a través de resoluciones del Consejo de Seguridad de las Naciones Unidas, sin embargo, una de las grandes dificultades que encontramos en este tipo específico de instancia es su carácter residual o subsidiario, y en palabras de Rodríguez Barrigón:

“El carácter internacional de los denominados Tribunales penales adhoc, esto es, los Tribunales Penales establecidos para la Antigua Yugoslavia y Ruanda queda fuera de toda discusión. Su origen se encuentra en resoluciones del Consejo de Seguridad de las Naciones Unidas dictadas sobre la base del Capítulo VII de la Carta. La interpretación de esta base jurídica como fundamento habilitante para que el Consejo de Seguridad pueda crear órganos subsidiarios de naturaleza judicial ha suscitado ciertas consideraciones sobre la validez de la misma, y más concretamente sobre la discrecionalidad del Consejo de Seguridad para adoptar medidas de esta naturaleza cuyos objetivos perseguidos pueden constituir una amenaza para la paz y seguridad internacionales.” (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)

Debemos tener claro entonces que la creación de estos tribunales nace en la Organización de las Naciones Unidas, sin embargo, actualmente no esta asociada a su competencia, sino que se delegó dicha potestad en el Consejo de Seguridad, el autor en cita plantea *“(...) la entidad de cualquier debate al respecto no está asociada a la capacidad de la Organización de Naciones Unidas para crear tribunales penales internacionales, sino que se derivó el mismo hacia las potestades del Consejo de Seguridad, y si éstas eran suficientes o adecuadas para establecer este tipo de órganos .”* (RODRÍGUEZ

BARRIGÓN, J. M., 2006 P. 334)⁶⁷². *Este tipo de consideraciones quedaron formalmente decididas por el Tribunal Penal Internacional para la Antigua Yugoslavia al resolver el Tribunal de apelación las cuestiones suscitadas en torno a la competencia del mismo para juzgar a Dusko Tadic, a quien se le imputaba la comisión de crímenes contra la humanidad, la violación de las leyes o costumbres de la guerra y de las Convenciones de Ginebra .”* (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 334)⁶⁷³.

Es claro que dentro de las funciones del Consejo de seguridad debe concentrarse la de creación de tribunales *ad hoc*, ya que es esta instancia la encargada del mantenimiento de la paz y la seguridad, bienes jurídicos tutelados que por su naturaleza deben ser resguardados por el Consejo de Seguridad, así lo determina. (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336) cuando dice: *Ciertamente, el acto creador de estos tribunales ad hoc tiene su razón de ser en las funciones propias del Consejo de Seguridad, no tanto porque el mismo ostente poderes de naturaleza judicial susceptibles de ser delegados a otros órganos, cuanto por el hecho de que el establecimiento de los mismos tiene como finalidad dotarse de un instrumento para el ejercicio de su función principal de mantenimiento de la paz y seguridad internacionales .* (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 335)⁶⁷⁴.

⁶⁷² Puede recordarse que la Resolución 827 (1993), manifiesta el convencimiento de que «en las circunstancias particulares que reinan en la ex Yugoslavia, la creación por el Consejo de un tribunal internacional, como medida *ad hoc*, y el enjuiciamiento de presuntos responsables de graves violaciones del Derecho internacional humanitario permitirían alcanzar este objetivo y contribuirían a la restauración y el mantenimiento de la paz. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitas P. 334.

⁶⁷³ Sentencia de 2 de octubre de 1995, dictada en el asunto *Prosecutor v. Dusko Tadic a/k/a «DULE»*, *Decisión on the Defence Motion for Interlocutory Appeal on jurisdiction*. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitas P. 334.

⁶⁷⁴ Sentencia -de 2 de octubre de 1995 del Tribunal Penal Internacional para la Antigua Yugoslavia, *cit. supra*, párrafos, 37 y 38. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos

La creación de los Tribunales internacionales, para el caso concreto de esta investigación, es decir, con el propósito de proteger a los ciudadanos del mundo de los ciberdelitos y conductas macrocriminales que ocurren en el ciberespacio, ha sido el avance más grande y significativo del Derecho Internacional, y ha constituido la base principal para desarrollar nuestra teoría de la Instalación de un Tribunal Internacional para la investigación, juzgamiento y sanción de los ciberdelitos, así mismo lo ha considerado Rodríguez Barrigón cuando dice:

“Con todo, la aportación de estos tribunales penales internacionales al desarrollo del Derecho Internacional no puede ser en modo alguno soslayada, pues teniendo como soporte una reacción de la Comunidad Internacional frente a crímenes internacionales, conlleva un importante progreso a la institucionalización de la sociedad internacional, lo que puede aventurarse como la mejor solución posible frente a violaciones graves de los Derechos Humanos y del Derecho humanitario (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)⁶⁷⁵.”

Sin embargo, aunque el concepto de Tribunal Internacional Ad Hoc, es el que permite el nacimiento de nuestra tesis, es indispensable aclarar que el alcance que pretendemos darle solo se logra invocando los presupuestos del Estatuto de Roma con la Creación de la Corte Penal Internacional, cuya competencia nace de la firma y aplicación de un convenio exclusivo para los Estados que deciden autónoma y libremente unirse. Más adelante nos referiremos a la

R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 335.

⁶⁷⁵ En este sentido, FERNÁNDEZ LIESA, C. R.: «El Tribunal para la Antigua Yugoslavia y el desarrollo del Derecho internacional», *Revista Española de Derecho Internacional*, Vol. XLVIII, 1996, núm. 2, pgs. 42-43.” **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

afectación que nos genera la característica de residual que posee este tribunal.

Vemos ahora en palabras del autor *ibídem* las diferencias entre los Tribunales Ad Hoc y la Corte Penal Internacional, así:

“Un carácter internacional indiscutible tiene también el Tribunal Penal Internacional. Su creación convencional y las particularidades de la estructura que se crea para dar soporte al mismo, revelan una naturaleza internacional claramente definida. Ahora bien, a diferencia de los Tribunales establecidos para las situaciones de Yugoslavia y Ruanda, su actuación queda limitada por la aplicación del Convenio de Roma exclusivamente a aquellos Estados que son parte en el mismo. Este hecho tiene consecuencias inmediatas sobre su actuación y marca diferencias sobresalientes con las obligaciones que se imponen a todos los Estados miembros de Naciones Unidas con las resoluciones del Consejo de Seguridad que establecen aquellos Tribunales ad hoc.

En esta línea, puede invocarse la inaplicación por parte de todos estos tribunales de del régimen general de la inmunidad de jurisdicción que es reconocida en el ámbito penal a ciertas personas que ostentan elevados rangos en los Estados, como son los Jefes de Estado, Jefes de Gobierno y los Ministros de Asuntos Exteriores, tal y como se dispone en las normas que los establecen, y que el propio Tribunal Internacional de Justicia ha reconocido como excepciones a la regla de inmunidad (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 335)⁶⁷⁶. Ahora

⁶⁷⁶ *Affaire relative au mandat d'arret du 11 avril 2000* (République Démocratique du Congo c. Belgique), Arrêt 14 février 2002, CIJ Recueil 2002, párrafo 61, pg. 25. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson civitas P. 336.

bien, la matización se impone, toda vez que la misma sólo podrá ser aplicada por el Tribunal Penal Internacional si los altos mandatarios requeridos lo son de un Estado parte en el Convenio de 1998.

Esta escueta descripción de los tribunales penales internacionales puede ser tomada como punto de referencia elemental para encontrar ciertas analogías y diferencias con otro tipo de tribunales que han ido surgiendo más recientemente en la Comunidad Internacional, con los que se amplía el espectro de jurisdicciones internacionales en materia penal". (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 336)

5.4.3. La creación de tribunales especiales.

Frente al tema de tribunales especiales, constituidos territorial y funcionalmente para un Estado en concreto, debemos referirnos obligatoriamente a los casos de Sierra Leona y el Líbano, bastante particulares porque aun cuando el objetivo de la creación de estos tribunales era para resolver conflictos que no sobrepasaron las fronteras territoriales, pero que su afectación a los bienes jurídicos tutelados de sus ciudadanos fue tan lesiva que la Organización de las Naciones Unidas se vio en la obligación, a través del Consejo de Seguridad, de intervenir dichos Estados para lograr el mantenimiento de la paz y la consecución de la justicia.

Juan Manuel Rodríguez Barrigón en su obra en cita, amplía nuestro conocimiento al respecto y nos permitimos citarlo, así:

Verdaderamente, las particularidades de los Tribunales Especiales constituidos para Sierra Leona⁶⁷⁷ y el Líbano⁶⁷⁸ deben ser objeto de una contextualización adecuada para comprender las motivaciones que han conducido a su establecimiento, y advertir las causas de los numerosos particularismos que los caracterizan. (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)

En el caso de Sierra Leona, el grave conflicto en que se vio envuelto desde 1991 arrojó escalofriantes cifras en cuanto al número de víctimas y exigió el desarrollo de una importante labor por parte de la ONU con vistas a contribuir a la estabilización de este país africano. Sin embargo, las atrocidades que se cometieron impulsaron la constitución, tras los Acuerdos de Paz de Lomé en 1999, de una «Comisión para la Verdad y la Reconciliación» cuya finalidad era crear un registro imparcial de los casos de violación de los Derechos Humanos y dirigir recomendaciones hacia el Gobierno con vistas a prevenir futuros conflictos. La preocupación por la situación de impunidad en que se estaban quedando los graves crímenes cometidos en este Estado contra su población y contra el personal de Naciones Unidas, impulsó al Consejo de Seguridad a instar al Secretario General a que negociara con el Gobierno de Sierra

⁶⁷⁷ Entre los diferentes estudios sobre este Tribunal Especial, pueden verse, entre otros, A. BLANC ARTEMIR: «El Tribunal especial para Sierra Leona: un instrumento contra la impunidad por las violaciones graves del Derecho internacional humanitario, *Anuario de Derecho Internacional* núm. 19, 2003, pgs. 101-138. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. *Tribunales Penales Internacionalizados: La especialización de la Justicia Penal*. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson civitasP. 336.

⁶⁷⁸ Los estudios publicados sobre este Tribunal aún pueden considerarse escasos, entre los que pueden verse A. AZAR: «Le tribunal spécial pour le Liban: une expérience originale?», *Revue générale de droit international public*, Vol. III, núm. 3, 2007, pgs. 643-658; W. SCHABAS: «Le Tribunal spécial pour le Liban fait-il partie de la catégorie de "certaines juridictions pénales internationales"?», *Revue québécoise de droit International*, 2006 (hors-série), pgs. 119- 132." **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. *Tribunales Penales Internacionalizados: La especialización de la Justicia Penal*. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Thomson civitasP. 337.

Leona un acuerdo para crear un Tribunal especial independiente con competencia para juzgar «los crímenes de lesa humanidad, los crímenes de guerra y otras violaciones graves del derecho internacional humanitario, así como respecto de los delitos tipificados en el derecho pertinente de Sierra Leona que hayan sido cometidos dentro del territorio de Sierra Leona» (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 336)⁶⁷⁹.

Las negociaciones entabladas por el Secretario General condujeron al Acuerdo entre las Naciones Unidas y el Gobierno de Sierra Leona acerca del establecimiento de un Tribunal Especial para Sierra Leona (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 336)⁶⁸⁰, por el cual se establece y se dota de un soporte normativo a un Tribunal con unos caracteres particulares que lo separan de otros tribunales penales establecidos hasta la fecha, como se tendrá ocasión de analizar más adelante. El acuerdo finalmente fue celebrado el 16 de enero de 2002 en Freetown, facilitándose su rápida ratificación y puesta en funcionamiento del Tribunal. (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 336)

Por su parte, el Tribunal Especial para el Líbano tiene su origen en el atentado con explosivos sufrido por el antiguo primer ministro libanés Rafiq Hariri el 14 de febrero de 2005, en el que falleció junto a una

⁶⁷⁹ Resolución 1315 (2000), de 14 de agosto de 2000. Este Acuerdo ha tenido algunos ajustes para adecuarlo a los objetivos marcados por el Consejo de Seguridad. Véase la Carta de fecha 12 de enero de 2001 dirigida al Presidente del Consejo de Seguridad por el Secretario General (S/2001/40). **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

⁶⁸⁰ El Acuerdo figura como anexo al Informe del Secretario General sobre el establecimiento de un tribunal especial para Sierra Leona, de 4 de octubre de 2000 (S/ 2000/915). **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

veintena de personas y en el que se registraron decenas de heridos. La situación que provocaba esta acción desencadenó una respuesta inmediata por parte del Consejo de Seguridad que subraya la grave incidencia que ha tenido este crimen sobre el inestable equilibrio del Líbano, y cuya trascendencia ha sido continuamente evocada (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)⁶⁸¹.

La calificación de este acto como terrorismo dio soporte a la creación de una Comisión Internacional Independiente de Investigación, a la que se asignó la misión de cooperar con las autoridades libanesas en la investigación de todos sus aspectos, incluida la identificación de sus autores, patrocinadores, organizadores y cómplices⁶⁸². Los informes emitidos por esta Comisión han prefijado algunos aspectos tendentes a determinar los elementos más relevantes de la ejecución de la acción terrorista y apuntan una cierta aproximación a la identidad de los implicados⁶⁸³, de tal modo que el Consejo de Seguridad ha adoptado la obligación para los Estados de adoptar ciertas medidas de aseguramiento sobre las personas designadas por la Comisión o el Gobierno del Líbano como sospechosas de estar involucradas en la

⁶⁸¹ Véanse las Resoluciones 1595-(2005), de 7 de abril de 2005; 1636 (2005) de 31 de octubre de 2005; 1644 (2005), de 15 de diciembre de 2005; 1664 (2006), de 29 de marzo de 2006; 1686 (2006), de 15 de junio de 2006; 1748 (2007), de 27 de marzo de 2007; 1757 (2007), de 30 de mayo de 2007; 1815 (2008), de 2 de junio de 2008. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

⁶⁸² Resolución 1595 (2005). En ella, además, se reclama al Gobierno libanés que someta a la justicia a los participantes en ese atentado. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

⁶⁸³ Los informes sucesivamente emitidos ponen de relieve la conexión entre este atentado y otras acciones, y la posible implicación de personas con nacionalidad libanesa y siria. Pueden verse en emitidos sucesivamente Informe Pueden verse Doc. S/ 2005/662, S/2005/775, S/2006/375, S/ 2007/150 y S/2008/210." **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 336.

comisión del atentado, consistentes en impedir el ingreso o tránsito en su territorio y la congelación de fondos, activos financieros y recursos económicos de las mismas (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)⁶⁸⁴.

La conexión de esta situación con el mantenimiento de la paz y seguridad en el Líbano son evidentes, especialmente si consideramos la fragilidad de las mismas en este país, por lo cual se atribuye una importancia especial a esta acción y la imperiosa necesidad de que no quede impune por la falta de eficacia de la actividad judicial libanesa. La propia Comisión de Investigación puso de manifiesto que la sumisión de la investigación y el ejercicio de acciones penales en el sistema judicial libanes se consideraba inconveniente dada su falta de credibilidad a los ojos de los ciudadanos, así como por la influencia que sobre el mismo podrían ejercer tanto los servicios de seguridad interiores como los sirios (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)⁶⁸⁵.

En estas condiciones, se apuntaron eventuales soluciones que condujeran a la eficaz investigación de los hechos y la sumisión de los autores a un tribunal penal. Ciertamente, las posibilidades que se abrían, y que fueron descartadas, apuntaban la necesidad de constituir un Tribunal especial, tal y como demandara el propio Gobierno

⁶⁸⁴ Como se dispone en la Resolución 1636 (2005), del Consejo de Seguridad que asimismo crea un Comité encargado de garantizar el cumplimiento de estas medidas y llevar el registro de personas señaladas. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 337.

⁶⁸⁵ Informe de la Comisión Internacional Independiente de Investigación establecida en virtud de la resolución 1595 (2005) del Consejo de Seguridad, de 19 de octubre de 2005 (Doc. S/2005/662). **Citado en** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 337.

libanes⁶⁸⁶. Para comprender esta decisión, debe tenerse presente que las posibilidades de constituir una nueva jurisdicción ad hoc no es fácilmente explicable si observamos que ya existía el Tribunal Penal Internacional, y no sería fácil justificar una nueva multiplicación de Tribunales con competencias similares. Ahora bien, no puede desconocerse que la sumisión de los asuntos que traen causa no podrían ser sometidos a este Tribunal, toda vez que el Líbano no es parte en el Estatuto de Roma y, además, la calificación de los hechos como terrorismo no encuentran acomodo entre las competencias materiales atribuidas a aquél. (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 336)

Ante estas circunstancias, el Consejo de Seguridad otorgó un mandato al Secretario General de las Naciones Unidas para abrir negociaciones con el Gobierno libanes que condujeron a un Acuerdo entre las Naciones Unidas y el Líbano relativo al establecimiento de un Tribunal Especial para el Líbano⁶⁸⁷. Las fuertes discrepancias internas que este acuerdo desencadenó impulsaron la adopción por el Consejo de Seguridad de una Resolución en la que se dispone con nitidez que las normas relativas al establecimiento de este Tribunal entrarán en vigor el día 10 de junio de 2007, si antes no ha notificado el Gobierno libanés

⁶⁸⁶ Como se reconoce en la Resolución 1644 (2005), que «pide al Secretario General que ayude al Gobierno del Líbano a determinar la naturaleza y el alcance de la asistencia internacional necesaria a este respecto, y pide también al Secretario General que presente oportunamente un informe al Consejo». **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. *Tribunales Penales Internacionalizados: La especialización de la Justicia Penal*. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Tomson civitasP. 337.

⁶⁸⁷ El texto puede encontrarse en el *Informe del Secretario General sobre el establecimiento de un tribunal especial para el Líbano* de 15 de noviembre de 2006 (S/2006/ 893). El Consejo de Ministros del Líbano había aprobado el Acuerdo el 13 de noviembre de 2006, abriéndose entonces un incierto camino para la ratificación.” **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. *Tribunales Penales Internacionalizados: La especialización de la Justicia Penal*. En: Carlos R. Fernández Liesa (Eds.) *Tribunales Internacionales y espacio Iberoamericano*. Madrid: Tomson civitasP. 337.

el cumplimiento de los requisitos legales establecidos en su orden jurídico interno⁶⁸⁸. En la medida en que el plazo expiró sin que se produjera la mencionada notificación, el inicio de su funcionamiento se debería fijar por el Secretario General en consulta con el Gobierno libanés, a la luz de los avances de los trabajos de la Comisión Internacional Independiente de Investigación. (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 337)

Como puede observarse, los Tribunales Especiales mencionados presentan unos rasgos comunes que los singularizan sobre el presupuesto de que su creación tiene un soporte convencional entre la Organización de las Naciones Unidas y los Estados para los que se establecen. Se apartan de este modo de aquellos Tribunales Penales Internacionales que se constituyeron para la Antigua Yugoslavia y Ruanda, para los cuales se recurrió al Capítulo VII de la Carta. Como se hará notar a continuación, esto tiene una notable influencia sobre el alcance normativo de los instrumentos que los regulan, pero también sobre las técnicas necesarias para alcanzar los objetivos perseguidos. (RODRÍGUEZ BARRIGÓN, J. M.,2006 P. 338)

5.4.3.1. Naturaleza de los tribunales especiales y sus competencias.

Para nuestro objeto de investigación en la presente tesis doctoral se hace indispensable el estudio de la naturaleza de los Tribunales Especiales y sus

⁶⁸⁸ Resolución 1757 (2007), de 30 de mayo de 2007. En anexo a esta resolución se contiene el Acuerdo entre el Secretario General de Naciones Unidas y el Gobierno del Líbano antes mencionado. **Citado en:** RODRÍGUEZ BARRIGÓN, J. M. 2006. Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Madrid: Thomson civitasP. 337.

competencias, recordemos que nuestra búsqueda investigativa va encaminada a encontrar un mecanismo que permita la investigación, juzgamiento y sanción de los ciberdelitos, es decir, aquellas conductas que sobrepasan las barreras territoriales de los Estados, de esta forma es imposible dejar de lado los aportes que la creación y establecimiento de Tribunales Ad Hoc ha dejado para el mundo del Derecho.

Rodríguez Barrigón define la naturaleza de estas instancias estableciendo que *la simple aproximación a las normas que establecen estos tribunales especiales invita a observar que las mismas parecen conformarse en unas fórmulas intermedias entre las utilizadas para los tribunales ad hoc y el Tribunal Penal Internacional.* (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 338). Estas fórmulas intermedias entre los tribunales ad hoc y el Tribunal Penal Internacional pueden generar confusiones a la hora de determinar su verdadera naturaleza, es por eso que el autor ibídem establece que *desde un punto de vista formal, al ser un Tratado internacional el que da soporte a la constitución de los mismos, su naturaleza internacional parece indiscutible; sin embargo, algunos de sus elementos definitorios apuntan a ciertos caracteres que inducen a plantear una hibridación con rasgos propios de los sistemas jurisdiccionales estatales.* (RODRÍGUEZ BARRIGÓN, J. M., 2006 P. 338)

5.5. Reglas jurídicas identificadas para prevenir el fraude en la contratación internacional: Autocontrol, tipificación, judicialización y cooperación nacional e Internacional

Con el curso investigativo desarrollado en la presente tesis doctoral se hace necesario traer a colación las Reglas Jurídicas identificadas para prevenir los

ciberdelitos, entre los que podemos encontrar el fraude en la contratación internacional, dichas reglas las he definido previamente dentro de la ponencia realizada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010, dentro de esta ponencia se logra identificar dichas reglas en: Autocontrol, tipificación, judicialización y cooperación nacional e Internacional, reproduciendo mi propia obra vemos:

Ante la necesidad de controlar las conductas ilícitas cometidas a través de medios electrónicos, puede decirse que existen dos posturas claramente identificadas; de un lado, una fuerte inclinación por su tipificación y con ella la ampliación en las funciones de policía judicial para la persecución del delito. De otro lado, se evidencia un contundente llamado, por parte de las multinacionales al autocontrol de los cibernautas y de las empresas que utilizan la red como medio para publicitar y/o distribuir sus productos. Algunas de las recomendaciones son las siguientes:

- *“Implementación de controles que impidan el acceso no autorizado a los servidores y computadoras. En el caso de una Compañía, por ejemplo, es conveniente que se restrinja el acceso físico a los servidores e instruir a los usuarios para que no divulguen sus contraseñas.*
- *“Definición de permisos de accesos según las funciones del personal dentro de la Compañía. A cada usuario se le otorgan permisos para poder realizar determinadas tareas, acceder a información sensible de acuerdo a su función dentro la Compañía. Por ejemplo, leer pero no modificar archivos o carpetas, utilizar o no la conexión a Internet, etc.*

- *“Ejecución de un plan de auditorías periódicas. Implementar un sistema de auditoría que permite guardar información relativa a lo que las personas hacen en un sistema informático. Esto permite luego monitorear las operaciones que un usuario ha realizado.*
- *“Uno de los retos más importantes en la lucha contra el delito informático es estimar su incidencia, su escala y su coste, que permita poder definir los tipos de medidas a adoptar y garantizar su proporcionalidad. En este sentido, leyes como Sarbanes-Oxley define a los ejecutivos como responsables de la seguridad informática al requerir que den su palabra de que los "controles internos" de las compañías son adecuados” (RINCÓN RÍOS, J. 2010)⁶⁸⁹.*

Un claro ejemplo de la descripción anterior, se tiene con Microsoft quien lanzó un portal sobre cibercrimen; en éste se incluyen diversos recursos de información, consejos y herramientas para investigadores. Al respecto Richard LaMagna, director de la unidad de los programas de aplicación legislativa de Microsoft, indicó que “(...) la compañía se quiere alinear con los esfuerzos emprendidos por las distintas administraciones para la persecución de actividades criminales” (RINCÓN RÍOS, J. 2010)⁶⁹⁰. Así, a través de una plataforma on-line, se brindan unas nociones sobre auditoría forense, soporte técnico, legislación vigente, de investigación on-line, con la finalidad de formar agentes implicados en la investigación.

⁶⁸⁹ Espiñeira Sheldon & Asociados, “El Delito Informático”, España, 25 de enero de 2007, <http://www.latinoseguridad.com/LatinoSeguridad/HCyP/delinfo.shtml>, página visitada abril de 2007. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

⁶⁹⁰ Hispasec Sistemas, “Microsof lanzará un portal sobre cibercrimen”, 6 de septiembre de 2005, <http://www.hispasec.com>, página visitada abril de 2007. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

Por su parte, el jurista colombiano Sergio Rodríguez Azuero indica que como respuesta frente al fraude en la contratación electrónica deben tenerse en cuenta la encriptación, la certificación y algunos instrumentos tecnológicos. (RINCÓN RÍOS, J. 2010)⁶⁹¹

La encriptación puede entenderse como “(...) un proceso que se vale de técnicas matemáticas para manipular el orden de los datos transmitidos, permitiendo que los mismos no puedan ser restablecidos a su forma original sin el conocimiento previo de una clave algorítmica” (RINCÓN RÍOS, J. 2010)⁶⁹².

Respecto la certificación, ésta “se presenta mediante la forma de una entidad que no es parte en la relación banco-cliente, que certifica el contenido de los mensajes y la veracidad del remitente, y que certifica el contenido de los mensajes de datos y la veracidad del remitente, función en virtud de la cual se busca superar los problemas de autenticidad. Con esta solución al riesgo operativo, se da seguridad a quien recibe el mensaje, para que pueda exigir posteriormente el cumplimiento de aquello que se convino mediante él” (RINCÓN RÍOS, J. 2010)⁶⁹³.

⁶⁹¹ Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

⁶⁹² Álvarez Álvarez, Julio Leñoso, citado por Rodríguez Azuero, Sergio, *op. cit.*, p. 110. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

⁶⁹³ Rodríguez Azuero, Sergio, *op. cit.*, p. 111. Subrayado fuera de texto. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

De lo expuesto en esta investigación se colige que el resultado de la misma deviene en la necesidad de crear un acuerdo jurídico global, que complemente los esfuerzos alcanzados en el Convenio sobre Ciberdelitos, en razón a las críticas aquí esbozadas, entre ellas, la insuficiencia del instrumento frente a la discrecionalidad de los Estados Partes para asumir todas las obligaciones en él expuestas, sumado a lo anterior, que no hace parte de una estrategia global, sino regional, en este sentido, se precisa una revisión de las condiciones de otros Estados para una reformulación de algunos tipos. (RINCÓN RÍOS, J. 2010)

Pensar en la formación de una norma internacional nos remite a entender varios aspectos; inicialmente, que constituye un proceso en el cual juegan especial preponderancia la coordinación de los intereses que motivan a los actores principales de la sociedad internacional. Dicha coordinación de intereses precisa de la negociación y posteriormente del consenso, del cual deviene entonces la norma internacional. (RINCÓN RÍOS, J. 2010)

Una norma internacional, en razón a que entre las funciones del Derecho Internacional, encontramos desde 1648 con la Paz de Westfalia, la necesidad de configurar la seguridad internacional. La historia de la sociedad internacional ha girado en torno al mismo aspecto: garantizar la seguridad y la paz mundial. (RINCÓN RÍOS, J. 2010)

El contexto actual, exige otro tipo de funciones complementarias del Derecho Internacional, entre ellas, la función ordenadora, la cual se encamina a la dirección de la conducta de los Estados para garantizar la convivencia pacífica; la función de cooperación, a través de la cual deben crearse

instrumentos de regulación, necesarios para superar los problemas globales, a través de convenciones de carácter universal. El crimen organizado global precisa de acuerdos entre la sociedad internacional, los cuales necesariamente deben estar regulados por el derecho internacional, puesto que en atención a su función teleológica debe procurarse por establecer la seguridad y la regulación de los conflictos (RINCÓN RÍOS, J. 2010)⁶⁹⁴.

En última instancia el derecho internacional hoy, más que nunca, precisa fortalecer su función sancionadora, relativa a la responsabilidad internacional de los individuos que amenazan y destruyen los acuerdos de civilidad firmados con sangre por la humanidad. Más aún, se requiere de la revisión de organismos intergubernamentales tales como la Corte Penal Internacional, si bien el Estatuto de Roma prescribe los más graves crímenes contra la comunidad internacional tales como el genocidio, crímenes de guerra, crímenes contra la humanidad y la agresión, enmarcados dentro del Derecho Internacional Humanitario y el Derecho Internacional de los Derechos Humanos. No fueron incluidos otro tipo de crímenes como la ciberdelincuencia, por obvias razones; el 17 de julio de 1998, el auge de este tipo de conductas aún no se había configurado como una amenaza de esta magnitud para la humanidad. (RINCÓN RÍOS, J. 2010)

Ahora bien; somos del parecer que la penalización no debe ser solamente por la comisión de conductas encaminadas a la agresión física como tal, sino también, de aquellas que se erigen contra los valores que sostienen la cultura

⁶⁹⁴ Terz, Panos – Pastrana Eduardo, “El Derecho Internacional al despuntar el siglo XXI”, un punto de vista sociológico del derecho internacional, Revista Papel Político, Bogotá, Colombia, Vol 12, No. 2 julio – diciembre, 2007, ISSN. 0122-4409, p. 541. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

de toda una civilización; por tal razón, debatir el tema del cibercrimen precisa de una discusión en cuanto a la graduación de los tipos; desde luego, no serán todos los delitos informáticos los que deban presentarse ante la jurisdicción de la Corte Penal Internacional. En todo caso, la necesidad de combatirlo, exige de la conformación tanto de un instrumento como de un tribunal internacional que erradique la impunidad del ciberespacio, y que, aproveche las iniciativas existentes, acondicionadas a las nuevas conductas, producto de la dinámica de una sociedad automatizada por la revolución de las TIC. (RINCÓN RÍOS, J. 2010)

Es por ello que nuestra propuesta se centra, de un lado en la negociación de un Protocolo adicional al Convenio sobre cibercrimen, que tenga por objeto el desarrollo de los elementos sancionatorios a nivel internacional, para aquellos responsables de este tipo de conductas, o, retomar el Estatuto de Roma, que en el artículo 121, hace alusión a la posibilidad de presentar enmiendas, siete años después de la entrada en vigor del instrumento; en ese caso la propuesta deberá ser presentada al Secretario General de las Naciones Unidas, con la finalidad de que la Asamblea de Estados Partes, decida si se examina la propuesta, para lo cual puede convocar a una Conferencia de Revisión (RINCÓN RÍOS, J. 2010)⁶⁹⁵

Un argumento adicional, para soportar nuestra posición frente a la necesidad de la tipificación de este tipo de conductas, en un instrumento internacional, es encontrado en un artículo de investigación publicado en la página web del Comité Internacional de la Cruz Roja; se hace énfasis en la guerra de la

⁶⁹⁵ Estatuto de Roma, artículo 123. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

información como herramienta empleada en los conflictos armados, se hace alusión allí al “ataque contra redes informáticas” o (Computer Network Attack, CNA), entendida esta conducta como toda operación cuya finalidad sea perturbar, negar, deteriorar o destruir la información contenida en ordenadores o en redes informáticas; este tipo de ataques son considerados como una nueva manera de llevar a cabo el combate, sostiene el autor que en este tipo de conductas, “el derecho humanitario es aplicable, habida cuenta de sus objetivos subyacentes, es decir, proteger a las personas que no participan directamente en las hostilidades, así como sus bienes. El derecho humanitario es aplicable cuando los ataques contra las redes informáticas tienden, o pueden, poner en peligro a personas o bienes protegidos, asimismo, dichos ataques incumben al jus in bello” (RINCÓN RÍOS, J. 2010)⁶⁹⁶.

El derecho internacional por tanto, como preocupación de los Estados, como sujetos principales, así como de otros actores del sistema internacional, que juegan un papel preponderante en el ciberespacio, deben encaminar sus discusiones a la reglamentación de tipos penales que sancionen estos medios y métodos nuevos de hacer la guerra.

Por tanto, y retomando al internacionalista Panos Terzs D. Sc., vale la pena recordar que el proceso de formación de una norma internacional atraviesa varias etapas: “primero se reconoce que existen determinados problemas tales como los problemas globales de la humanidad, problemas concretos de las relaciones económicas internacionales etc. Sobre esto surge paulatinamente un consenso general (consensus generalis), o incluso un

⁶⁹⁶. Schmitt Michael N, op. cit. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

consenso de todos los estados (consensus ominium). Ya en la parte cognoscitiva del consenso de los estados, toman parte en su complejidad una serie de determinantes (ideales, económicos, ideológicos, internos de estados e internacionales). Ellos condicionan en su conjunto los intereses del estado. (RINCÓN RÍOS, J. 2010)

“Después de esto es reconocido, por uno o varios Estados, por las mismas o similares razones, el significado de los problemas en cuestión. Sobre esto puede existir un consensus generalis o incluso un consensus omnium; según sea el caso. El grado de significación del problema es, sin embargo, dependiente del concreto grado de intereses de los correspondientes estados. (RINCÓN RÍOS, J. 2010)

“La comprensión de los problemas existentes en la realidad objetiva está unida, en lo referente a su significación, a una valoración. A ella le sirven de base factores que se arraigan en las condiciones de vida material, o bien se encuentran en la superestructura. A través de la percepción, conocimiento y valoración de los problemas, llegan los estados a la necesidad de reglamentación y dignificación de una norma.

“(…)

“En este proceso participan tales factores como la conciencia jurídica y el sentido de justicia. Cuando varios Estados reconocen la necesidad y la posibilidad de crear una norma y, que tal hecho es digno de ser normado, entonces se puede afirmar la existencia de un consensus omnium. En esta fase los estados interesados establecen contactos entre sí para reglamentar los problemas en cuestión.

“Después de esto se extiende el consensus de los Estados a los problemas, de procedimiento a calificar. Esto se obtiene mediante negociaciones y compromisos mutuos.

“(…)

“Durante el proceso de negociaciones los estados tratan de lograr un equilibrio de intereses. En esto toma parte una amplia gama de determinantes: Los problemas globales de la humanidad, la correlación internacional de fuerzas, bajo determinadas circunstancias las obligaciones que impliquen ser miembro de un determinado pacto, la independencia, la opinión pública internacional, la posición ideológica y política de los Estados, el potencial económico, la situación geográfica, la situación política interna de un Estado, las concepciones jurídicas, los valores, la expectación, etc. Estos factores producen sus efectos en forma compleja y generalmente simultánea. Estos forman parte de un proceso dialéctico y contradictorio. (RINCÓN RÍOS, J. 2010)

“En el proceso de negociaciones los Estados coordinan sus intereses, las voluntades y deseos basados en ellos y sus opiniones y las que estén influidas por los mencionados intereses. El resultado de este procedimiento es la expresión del consenso en referencia a causa y contenido y se reflejan en tratados, declaraciones, resoluciones de la Asamblea General de la ONU (...) y representa, desde el punto de vista teórico del proceso de formación de las normas, reglas de conducta”⁶⁹⁷. Frente a lo cual los estados deciden si serán normas de carácter jurídico o no jurídico, así como, para el primer caso, las

⁶⁹⁷ Terz, Panos, “Cuestiones teóricas fundamentales del proceso de formación de las Normas Internacionales”, ed. Universidad Santiago de Cali, Santiago de Cali, 1999, p. 64. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

reservas que pueden ser: jurídicas, políticas o morales (RINCÓN RÍOS, J. 2010)⁶⁹⁸.

En el Capítulo cuarto analizamos el Convenio sobre Ciberdelito, único instrumento internacional que reglamenta la posible tipificación penal de este tipo de conductas, así como la parte procedimental, a cargo de las autoridades para perseguir el delito. No obstante, señalábamos que si bien, valoramos esta importante iniciativa propuesta por la UE, también hemos dicho que consideramos se precisa de un instrumento coercitivo generador de acuerdos, un Protocolo adicional, por ejemplo, que contenga unos parámetros iguales para todos los Estados que lo suscriban; en otras palabras, el Convenio sobre Ciberdelito, es un acuerdo macro, es decir, en él se presenta una directriz a seguir, pero igual queda a discrecionalidad de los Estados asumir todos los compromisos allí sugeridos.

Según el análisis del proceso de formación de la norma internacional propuesto por el profesor Terz, el sistema de Estados ya ha reconocido la existencia de un problema de dimensiones considerables, puesto que la Internet se convirtió en un excelente canal para la actuación de la criminalidad organizada; la sustentación de esta investigación se ha tejido a partir de argumentos en los cuales se presenta cómo las plataformas electrónicas sirven de soporte para diferentes actividades ilegales, atentatorias de valores esenciales para la proyección de la humanidad, que si bien, han existido desde antes, ahora cobran mayor fuerza dada la facilidad que les proveen los medios electrónicos.

⁶⁹⁸ Cfr. Ibídem, p. 69. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

Por lo tanto, no se trata solamente de establecer el lugar de perfeccionamiento de un contrato celebrado por este medio, con la finalidad de identificar el momento en que comienza a generarse la prestación; ese es solamente un aspecto importante, que se relaciona con la seguridad jurídica y el comercio electrónico, pero la cuestión va mucho más allá; las redes sobre la pornografía infantil, el tráfico de drogas y el acceso mucho más fácil de las personas a él, a través de la compra virtual, constituyen claros ejemplos; o de otro lado, la estafa informática y la pérdida de muchísimo dinero tanto para personas naturales como jurídicas, así como la violación a la intimidad que va a gran escala, no solamente para identificar los gustos de un cibernauta, sino como espionaje industrial a grandes emporios privados o a dependencias estatales. En últimas, porque el flagelo del cibercrimen se constituye en una contundente amenaza contra la economía digital, que debe entenderse como la nueva economía globalizante y, por ende, necesita de una continuación del Convenio sobre Cibercrimen; pero en este caso, no se trata de suscribir un acuerdo macro sino un acuerdo multilateral, un Protocolo adicional, con obligaciones bien definidas y homogéneas para todos los Estados Parte. (RINCÓN RÍOS, J. 2010)

La sociedad del conocimiento irguió sus cimientos sobre el desarrollo del saber y la aplicación de la tecnología, para resolver los problemas y hacer más fácil la vida humana. Sin embargo, la dimensión cobrada por las actividades ilegales, valiéndose del mismo avance de la ciencia, desborda cualquier intento por atacar este fenómeno con paliativos. Se precisa por tanto de una estrategia fuerte, encaminada a salvaguardar la seguridad de los habitantes del mundo, una seguridad que debe entenderse a partir de la complejidad que implica el ser humano, desde lo cultural, y es velar por el sistema axiológico, soporte cultural de la especie humana. De lo anterior, se desprenden toda una serie de cuestiones también importantes como la

transparencia y la seguridad para comprar y vender en la red, la protección de la intimidad a pequeña y gran escala, y, por encima de todo, la defensa de la dignidad humana contra la cual se atenta desde la red, entre otros aspectos que aparecen producto de los cambios vertiginosos.

El entorno actual se caracteriza por el aumento de la delincuencia organizada a todo nivel; según Jaume Curbet los poderes públicos son impotentes ante la nueva criminalidad organizada; por tanto, los gobiernos terminan arrodillados o sustituidos por las organizaciones criminales, las cuales controlan la riqueza a través de la violencia y la coacción. “No es difícil, pues, pronosticar que el creciente poder de estas organizaciones posestatales terminará desafiando si es que no la ha hecho ya al Estado convencional mediante el establecimiento de diversos vínculos mercenarios transnacionales y defenderán, cada vez más, ambiciones regionales e incluso mundiales” (RINCÓN RÍOS, J. 2010)⁶⁹⁹.

Este panorama exige una acción contundente que quizá se entienda como la expansión del derecho penal internacional, la cual precisa de un sustento teórico encaminado a combatir la impunidad del ciberespacio. No obstante, queremos advertir que su presentación no implica necesariamente nuestra adhesión; consideramos que puede sustentar una propuesta de política criminal, en cuanto la necesidad de fundamentar la tipificación de esta serie de conductas atentatorias del orden jurídico nacional e internacional, por su calidad de ser transfronterizos, a cargo de la criminalidad organizada.

⁶⁹⁹ Curbet Jaume, “La glocalización de la (in)seguridad”, ed. Plural editores, primer edición, Madrid, 2006, p. 27. Citado en Rincón Ríos, J. 2010. Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.

En este sentido, intentar perseguir el cibercrimen organizado, implica una intromisión de la autoridad en la esfera personal del individuo, la cual se encontraría justificada por el daño potencial en el que se encuentra permanentemente la sociedad, y el Estado tiene la posición de garante como responsable, siendo la corte penal internacional una solución viable, que impide un desbordamiento del criterio de la sanción penal. (RINCÓN RÍOS, J. 2010)

5.6. EL DELITO UBICUO O GLOBAL, COMO DESARROLLO DEL PRINCIPIO DE UNIVERSALIDAD. OTRA SALIDA A LA DELINCUENCIA MUNDIAL ELECTRÓNICA.

5.6.1. El Delito Informático como motor de cambios conceptuales en el Derecho Penal.

5.6.1.1. Necesidad de cambios conceptuales en el Derecho Penal

Es en este acápite investigativo donde nos dedicaremos a resolver lo que en un primer momento metodológico definimos como problema de investigación, y es precisamente tomando como referencia los grandes aportes de mi Maestro Emilio Suñé Llinás dentro de su teoría del delito UBICUO, que logramos dilucidar un modelo que permitiría por lo menos de forma transitoria la investigación, juzgamiento y sanción de los cibercrímenes o ciberdelitos dentro del marco del derecho penal internacional.

Para empezar el abordaje dogmático y en sí el desarrollo de esta tesis doctoral debemos identificar lo que conocemos inicialmente como ciberdelitos, remitiéndonos al Maestro Suñé Llinás, cuando nos dice:

“Al existir la conciencia de que más que nuevas formas de delinquir, la tecnología suele ofrecer nuevas posibilidades para la comisión de lo que, a fin de cuentas, son delitos tradicionales. A mi modesto entender, esta conciencia hace que existan menos reticencias a admitir la interpretación extensiva de los tipos penales, sobre todo si dicha interpretación se lleva a cabo de forma medida y se minimizan los riesgos de confundirla con la analogía in malam partem que, también a mi juicio, debe seguir siendo una técnica interpretativa proscrita, en el ámbito del Derecho Penal. SUÑE LLINAS, E., 2001⁷⁰⁰.”

Entonces vemos que en su gran mayoría, los doctrinantes del derecho penal le han impuesto una característica de novedosa a los delitos a través de los medios informáticos y las tecnologías de la información y las comunicaciones, dándole una interpretación extensiva a los tipos penales “tradicionales”, a nuestro modo de ver, lo que realmente debe tenerse en cuenta es la diferencia dogmática de los delitos informáticos per se, y aquellos en los cuales la modalidad de comisión se encuentra enmarcada dentro de los mecanismos informáticos, electrónicos y de las telecomunicaciones.

Es esta construcción teórica la que nos permite dar paso al segundo eje temático desarrollado por el Doctor Suñe Llinas y es el de la consideración de que algunos tipos penales se constituyen como delitos globales, así lo establece el citado maestro, cuando dice:

“La segunda cuestión que integra el presente estudio hace referencia asimismo a una cuestión novedosa, cual es la del delito global; o lo que es lo mismo, aquel delito que se comete en todo el mundo a la vez, con

⁷⁰⁰ SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

la consiguiente crisis radical del principio de territorialidad del Derecho Penal y que requiere a mi juicio de respuestas igualmente radicales, hasta el punto de que propugno que pueda ser perseguido desde cualquier país del orbe en el que los correspondientes hechos estén efectivamente tipificados como delitos. El supuesto paradigmático es el de la difusión de pornografía infantil a través de Internet y es muy distinto a los supuestos de jurisdicción universal ante delitos como el de genocidio. En este último caso existe una jurisdicción universal por consideraciones estrictamente jurídicas, vinculadas a determinadas clases de ilícitos penales, que se consideran como delitos contra la humanidad, mientras que el problema que en el presente estudio se menciona es el de jurisdicción universal como consecuencia de consideraciones fácticas y no jurídicas, no en vano, en determinados supuestos, como el de pornografía infantil distribuida a través de la red, el delito puede estar cometiéndose allá donde la correspondiente conducta esté tipificada y el material indecente y execrable se halle disponible. Virtualmente, en todo el mundo a la vez. En estos casos, reitero, la crisis del principio de territorialidad del Derecho Penal, no obedece ya a razones jurídicas, basadas en el delito de que se trate, sino en consideraciones fácticas derivadas de que el delito se está cometiendo en muchos países a la vez. (SUÑE LLINAS, E., 2001.)

El concepto de delito global o delito UBICUO, desarrollado por el autor citado anteriormente se ha convertido en el insumo principal para el desarrollo de esta investigación, puesto que los delitos, que al momento de ejecución de la conducta que permite tipificarlos, se realizan a través del ciberespacio, es decir, palpables desde diferentes lugares en un mismo momento generan un grave conflicto para su adecuación típica, antijurídica y culpable (dentro de la teoría finalista del delito), esto debido a su factor territorial lo que genera mayores dificultades respecto a su persecución y las diferencias legislativas entre los

estados (donde se ha podido identificar la comisión del ilícito) pueden resultar en responsables de impunidad, adicionalmente a esta situación, nos encontramos con que los grandes especialistas del Derecho Penal, no suelen ser los mismos expertos en informática, quienes serían los indicados, por lo menos, para la fase de investigación del delito.

En este sentido continuamos con lo evidenciado en la obra del Doctor Suñé:

“Puede parecer un tanto extraño que me adentre en cuestiones tan polémicas sin ser, ni de lejos, un especialista en Derecho Penal. Sustancialmente me atrevo a hacerlo por algo que ya expresé en el Volumen I de mi Tratado de Derecho Informático, al referirme a dicha disciplina, en cuanto rama del Derecho. Entonces dije y ahora ratifico lo siguiente: Si bien es de todo punto imprescindible que existan especialistas en Derecho de la Informática, ello no implica que estos deban prescindir, sino antes bien fomentar, la colaboración con los especialistas de las ramas que hemos denominado verticales del Derecho -y, por supuesto, también viceversa-. Los especialistas auténticos en Derecho de la Informática tienen la perspectiva y la formación tecnológica; pero no pueden ser omniscientes, ni siquiera en el exclusivo ámbito del Derecho, que hoy en día está muy especializado en sus ramas tradicionales. De ahí que, a salvo la sustantividad del Derecho de la Informática, es bueno que los civilistas no dejen de prestar atención a la protección jurídica del software, los mercantilistas a las repercusiones jurídicas del comercio telemático, por ejemplo, los laboristas al teletrabajo, o los penalistas al delito informático; pero siempre teniendo en cuenta que se entra en materias que requieren de un conocimiento técnico sólido, una visión de conjunto y una perspectiva innovadora, que sólo puede derivar de la especial cualificación de los

auténticos especialistas en Derecho de la Informática. SUÑE LLINAS, E., 2001.

5.6.1.2. Uso de medios tecnológicos como agravante de los tipos penales tradicionales

Las dificultades conceptuales creadas en gran parte por los doctrinantes tradicionales del Derecho penal, han llevado a que las legislaciones antes de lograr generar cambios definitivos en la concepción de nuevos tipos penales dentro del orden cibernético o informático y de las telecomunicaciones, se hayan dedicado primero a considerar como agravantes punitivos el uso de los medios informáticos, electrónicos y de las telecomunicaciones dentro de la comisión de los delitos tradicionales, dejando esta situación en condición de mayor inferioridad a la víctima y así lo establece nuestro principal referente bibliográfico tomando como ejemplo la legislación española:

“(..) a nivel de modificaciones legislativas, no propugno tanto introducir nuevos tipos penales, lo cual, en general, es una cuestión mucho menos importante que el cambio de mentalidad interpretativa, como el hecho de que el legislador pase a considerar como agravante genérica el hecho de ayudarse para la realización de cualquier delito con medios tecnológicos -no sólo informáticos- que sitúen a la víctima en clara inferioridad frente al ofensor. Esta alternativa casa perfectamente con la tradicional idea de superioridad que late en exactamente la mitad de las agravantes genéricas enumeradas en el artículo 22 del Código Penal Español de 1995, y más en concreto:

- a) *Alevosía.*
- b) *Abuso de superioridad.*
- c) *Abuso de confianza.*
- d) *Prevalerse de carácter público. (SUÑE LLINÁS, E., 2001.)⁷⁰¹*

5.6.1.3. Interpretación extensiva de los tipos penales.

Claramente para las legislaciones positivistas como es el caso Español y el Colombiano, es, además de complicada, lenta y dotada de formalismos la expedición de nuevos tipos penales que pueden implicar cambios mayores dentro de la estructura penal dogmática de cada Estado, razón por la cual, es mucho más práctico acudir al criterio de interpretación penal *extensiva*⁷⁰², donde podrá lograrse, al menos someramente, que las legislaciones no se queden tan atrasadas frente a los avances sociales, tecnológicos y culturales, así lo cita el Doctor Suñé Llinas, explicándonos como la interpretación extensiva se reduce a los elementos estrictos del hecho que han sido utilizados para la comisión del injusto, haciendo así, que si positivamente se regula la interpretación extensiva para estos casos de ciberdelitos o sea mucho más práctico para los Estados, circunscribirse al nuevo Tratado de Derecho Penal Internacional que pretendemos como solución al nuestro problema de investigación, y generar acciones concretas encaminadas a la consecución de la justicia y reivindicación a las víctimas. Las palabras exactas del Honorable Doctor Suñé Llinás al respecto son:

⁷⁰¹ SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

⁷⁰² SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

“Por lo demás, he de insistir en que, por lo común, no surgen tanto nuevos delitos, como nuevas formas de cometer delitos previamente tipificados, por lo que, en la mayoría de las ocasiones bastaría con no poner excesivos reparos a la interpretación extensiva de los tipos tradicionales, máxime cuando ni siquiera hace falta que ésta alcance a todo el tipo, sino exclusivamente a los elementos de hecho que se emplean para la comisión del delito. De no procederse así, se puede pronosticar, sin demasiado riesgo de equivocarse, que ante un avance tecnológico de la magnitud del que se da en las actuales coordenadas históricas, el Derecho Penal está condenado a un permanente desfase en relación con las nuevas formas de delinquir, de tal forma que van a escapar de su ámbito, por estrictas razones formales, muchos hechos que repugnan a la conciencia social y a los propios Códigos Penales. Si, como se acaba de afirmar, la interpretación extensiva se reduce a los estrictos elementos de hecho empleados para la comisión del delito, respetándose, en todo lo demás, el tipo stricto sensu, apenas si aparece el riesgo de arbitrariedad -y menos en un Estado de Derecho, con Poder Judicial independiente- o de abrir una puerta falsa a la analogía in malam partem. (SUÑE LLINÁS, E., 2001.)⁷⁰³”

5.6.1.4. Diferencia entre analogía e interpretación extensiva

Citando nuevamente al doctor Suñe Llinás, encontramos como las fuentes de interpretación del derecho penal, tal y como están definidas actualmente permiten, en palabras del autor, dar el alcance necesario para que sea un organismo universal el encargado de proteger los bienes jurídicos nacientes en la sociedad de la información, creando una jerarquización diferente a los

⁷⁰³ SUÑE LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

principios generales para la interpretación del derecho de forma que, para el Maestro español, sería la analogía el primer modelo y no la interpretación extensiva, a pesar de que en la práctica jurídica pueda ser mas fácil utilizar el segundo, como se planteó en el acápite anterior, a continuación citamos la conclusión a la cual ha llegado el Distinguido autor en cita:

El criterio diferenciador más nítido entre analogía e interpretación extensiva, estriba en que la analogía se basa en extraer los principios que informan la regulación de uno o varios supuestos normados, para aplicarlos después a casos que guardan identidad de razón con los previstos en aquellas normas. La interpretación extensiva, en cambio, afecta más a la disposición que a la norma propiamente dicha; pues no trata de alumbrar una nueva norma a través de la inducción de principios generales del Derecho, a partir de otra u otras normas expresas, sino de rebasar una interpretación de tipo estrictamente declarativo de una norma expresa. La interpretación extensiva no deja de ser una variedad de la literal, con el matiz de que los términos en que está redactada la correspondiente disposición se interpretan en sentido amplio y no meramente declarativo. (SUÑE LLINÁS, E., 2001.)⁷⁰⁴

Finalizando la diferencia entre la Interpretación extensiva y la Analogía, el Maestro Suñé nos dice que, la interpretación extensiva forma parte de la interpretación literal, mientras que la analogía se inscribe entre los diversos tipos de argumentación que integran el criterio lógico de interpretación. (SUÑE LLINÁS, E., 2001.)

⁷⁰⁴ SUÑE LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

Es esta concepción de la Analogía elaborada por el Maestro Suñé, elabora una diferencia conceptual con el principio de Analogía prohibido por los principios generales del Derecho, donde se compone de un método argumentativo complejo que para los casos de ciberdelitos, investigados y juzgados dentro de un tribunal internacional no constituiría una afectación al presupuesto de la tipicidad de la conductas. Es así como los Estados que pretendan hacerse miembros, podrán dar seguridad jurídica a las víctimas a quienes se les han vulnerado sus bienes jurídicos tutelados, evitando el flagrante riesgo de vulnerar el debido proceso de los agresores, situación de gran connotación jurídica y social, puesto que es la primera característica que poseen dichos tribunales y en sí es la razón por la cual los Estados depositan su confianza jurídica en estas instancias internacionales.

5.6.1.5. Principio territorial y personal

Aclarado el punto de como el modelo jurídico internacional planteado en la presente investigación abordará la problemática de la interpretación de las conductas consideradas como punibles, es necesario dar paso al debate frente a la territorialidad y personalidad penal como principios del Derecho Penal, así lo ha planteado el Doctor Suñé Llinás:

El Derecho Penal, como sucede con la práctica totalidad de las ramas del Derecho, se mueve en la tensión entre los principios territorial y personal, si bien este último principio, pesa menos aquí que en otras ramas del Derecho, por la usual vinculación del orden público estatal al principio de territorialidad. (SUÑÉ LLINÁS, E., 2001)

El principio personal ha tenido, sin duda, un carácter excepcional en el Derecho Penal, incluso desde el punto de vista histórico, puesto que ha

*estado tradicionalmente vinculado a las particulares características del Derecho Germánico. Conforme señalaba el argentino Carlos Alberto Alcorta, el Derecho Penal Germánico antiguo, en cuanto “derecho de las razas”, entendía a todos los efectos que la condición jurídica de la persona se regía por la ley propia de la raza o tribu a la que pertenecía, hasta tal punto que, ante hechos punibles cometidos por extranjeros, se respetaba también la aplicación del Derecho punitivo del correspondiente pueblo no germánico*⁷⁰⁵.(SUÑE LLINÁS, E., 2001)⁷⁰⁶

Es necesario entonces, dar un nuevo alcance a este principio de personalidad penal, entendiéndose éste como la pertenencia de la persona a la raza humana y alejándose de la concepción según la cual cada estado es soberano para la persecución penal de las conductas que considere atentativas a los bienes jurídicos tutelados. en estos casos la apreciación de juzgamiento y condena no puede depender del lugar donde se realice la conducta, puesto que la sociedad de la información y la globalización permiten que dicha comisión se realice desde cualquier lugar del mundo, atentando contra intereses jurídicos objeto de protección diferente por cada estado, razón por la cual se hace necesario un órgano universal, que proteja de manera concreta los bienes vulnerados y que no se vea limitada esta política criminal a los ordenamientos nacionales, por el contrario, que sean estos quienes en concordancia con el órgano universal permitan la ejecución de dicha política como protectora de las víctimas, que en este tipo de delitos puede ser el mismo estado, es así como se configura la teoría del delito global.

⁷⁰⁵ C. A. Alcorta, *Principios de Derecho Penal Internacional*, ed. Italia, Buenos Aires (Argentina), 1931. Pág. 47. Citado en : SUÑE LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

⁷⁰⁶ SUÑE LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

El autor citado y guía de esta investigación nos muestra como el principio de territorialidad no es un concepto nuevo, al contrario, obedece a desarrollos jurídicos ancestrales que permiten su implementación para este caso concreto, *el principio de territorialidad, en ocasiones cedía el paso al de universalidad cuando el poder de los grandes imperios lo hacía posible. Ello se vio tanto en los países anglosajones, como en la expansión imperial española. El Reino Unido amparaba a sus propios corsarios, defendía un poder exterior no sujeto a las leyes, con la idea del poder federativo, que aparece hasta en la intachablemente liberal obra de Locke, e incluso consiguió que el Congreso de Viena de 1814 aprobase un orden público internacional contrario a la esclavitud que bienvenido fuese, a pesar de que iba destinado a obtener pretextos para la interceptación de barcos negreros españoles y portugueses, potencias a las que Inglaterra pretendía perjudicar, una vez que ella ya había perdido sus colonias en Norteamérica y no necesitaba, en consecuencia, mano de obra esclava. Y qué decir del episodio del Rajá de Benarés, relatado por Burke, que da fe de la aplicación imperialista del Derecho Penal propio en las colonias británicas. Montesquieu atribuyó este mal al Imperio Español, en el lamentable episodio del asesinato del Inca Atahualpa[20]; pero, como vemos, fue mal común a todos los imperios coloniales, sobre todo cuando eran de envergadura, lo que - probablemente a su pesar- nunca fue el caso del imperio colonial francés. (SUÑÉ LLINÁS, E., 2001)⁷⁰⁷*

Continúan las citas bibliográficas al respecto:

“En mérito de España, hay que decir que en pleno apogeo de su Imperio colonial, siempre produjo vástagos con profundos sentimientos

⁷⁰⁷ SUÑÉ LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

humanitarios, desde la época inicial de la polémica sobre las Indias, hasta -y después- de los tiempos señeros de Covarrubias y Francisco Suárez, que vieron en los crímenes más abominables, una violación del orden jurídico natural de la societas generis humani. Ello no fue mérito exclusivo de algunos españoles, pues también Grocio⁷⁰⁸ y Wolff⁷⁰⁹, defendieron el principio universal con parecidos argumentos.

No hay que perder de vista, especialmente, la advertencia de Wolff, según la cual, si bien hay que clamar por el principio de universalidad del Derecho Penal, ante las violaciones más graves del Derecho Natural, no por ello se debe eliminar su vinculación ordinaria a la soberanía del Estado. Algunos siglos después, pienso más o menos lo mismo, por muchas razones, entre ellas que el principio de territorialidad del Derecho Penal es una prerrogativa del Estado, pero también una garantía para los ciudadanos de todo el orbe, pues si los Estados ejercieran ordinariamente su potestad para establecer y perseguir delitos más allá de las propias fronteras, todos tendríamos la inquietud de poder vernos sometidos, en cualquier momento y por las circunstancias más variopintas, a la potestas

⁷⁰⁸ Grocio, en *De Iure Belli ac Pacis*, Libro II, Cap. XX, § 40, nº 1, dice: *También debe saberse que los reyes y quienes tienen derechos iguales al de los mismos, poseen la facultad de exigir el cumplimiento de las penas, no solamente por agravios e injurias cometidos contra ellos o sus súbditos, sino también por actos que a ellos personalmente no afectan y en cualquier sujeto que viole gravemente el derecho natural o el derecho de gentes.* Citado en: SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

⁷⁰⁹ De Wolff, dice Carlos Alcorta: *Ratifica conceptos cosmopolíticos de Grotius, adhiriendo a la tesis de una ley superior -derecho natural- que gobierna al universo y que considera como propia de la "Civitas Maxima" que se extiende en todas las partes del mundo con el mismo imperio y poder. La ley penal en el sistema de Wolff se identifica así en la natural organización de la humanidad que queda afectada con los hechos delictuosos cometidos en un lugar determinado y, por consecuencia sistemática, en el dominio del universo; pero advierte la intención de no eliminar en materia penal, las cuestiones que se originan por causa de las soberanías territorial y personal de los Estados.* C. A. Alcorta, op. cit. Pág. 69. Citado en: SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

puniendi de cualquier Estado, como le sucedió a Rushdie con la fatwa de Jomeini (SUÑÉ LLINÁS, E., 2001).

Así concluye el doctor Suñe cómo el derecho penal desde una óptica universal debe componerse, entre otros, de los principios de territorialidad y universalidad, definiendo, para los delitos de carácter trasnacional una interpretación principialística diferente a la de los delitos que competen únicamente la órbita de soberanía de los estados, y esquematiza la aplicación del principio de universalidad así:

“El principio de universalidad, conforme hemos visto, puede ser esgrimido por laudables razones humanitarias; pero también es susceptible de generar efectos perversos de tipo imperialista, cuando no de someter a ciudadanos de los países libres al capricho del fanatismo y la barbarie. En todo caso, hoy en día, hay que prestar especial atención al principio universal, que es el que mejor puede permitir atajar la delincuencia internacional y los nuevos delitos globales. Sólo con un Derecho Internacional Penal eficaz, será posible poner coto a delitos tales como el narcotráfico, tráfico de armas, lavado de dinero, esclavitud sexual y otras conductas igualmente detestables, que promueven las multinacionales del crimen. (SUÑÉ LLINÁS, E., 2001)”

Es entonces según el planteamiento anterior que podemos dar una aplicación real y material del principio de universalidad a los ciberdelitos, recordando que sin importar el lugar donde inicie la ejecución de la conducta punible, cuando esta conducta atenta bienes jurídicos tutelados por otros Estados y territorios, se ha convertido en un delito trasnacional, que debe ser juzgado bajo los

parámetros del Derecho Internacional y que cuenta con la aplicación del principio de universalidad.

5.6.1.6. Principios supraterritoriales

Es importante al adelantar esta investigación doctoral, destacar el gran aporte del Maestro Suñé Llinás al respecto de la creación de un mecanismo de persecución Penal Internacional, es por esto que nos permitimos traer a colación los planteamientos de la realidad política y jurídica que nos ha dejado el Doctor SUÑÉ LLINÁS, así:

“Conviene recordar que los principios territorial y personal no son los únicos relevantes para la precisión del ámbito de aplicación del Derecho Penal, puesto que en ocasiones hay que traer a colación principios supraterritoriales, como el real y el de jurisdicción universal. El principio real extiende la jurisdicción de un Estado más allá de su territorio, por razón de la materia concreta vulnerada. Como señala Antonio Quintano Ripollés, el principio de jurisdicción universal se distingue del real, en que el primero atiende a intereses comunes a la humanidad, mientras que el segundo se refiere a intereses básicos del Estado. Por esta misma razón, el principio de jurisdicción universal suele establecerse en Tratados Internacionales, mientras que el principio real suele establecerse unilateralmente por cada Estado⁷¹⁰ (SUÑÉ LLINÁS, E., 2001)

⁷¹⁰ Quintano Ripollés, *Tratado de Derecho Penal Internacional e Internacional Penal*, Tomo II. Ed. vPág 101. Citado en: SUÑÉ LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

No obstante, cuando el principio de jurisdicción universal se establece por consideraciones imperialistas, se difumina su distinción con el principio real, pues ambos acaban sirviendo los estrictos intereses del Estado. Así por ejemplo, en este gran punto de referencia para el Derecho, que fue Roma, prevaleció el principio de jurisdicción universal, que, como se acaba de decir, puede tener un carácter decididamente imperialista, cuando un ente político dotado del suficiente poder decide que todo lo que afecte a su territorio, ciudadanos e intereses, queda sometido a sus normas y jurisdicción punitiva; pero no por el carácter imperialista del principio de universalidad del Derecho Penal Romano, deja de ser cierto que cuando el punto de referencia es la común naturaleza humana y los Derechos del Hombre, el principio universal puede ser defendido por razones bien distintas y en todo caso plausibles. Más adelante se volverá sobre este tema. (SUÑÉ LLINÁS, E., 2001)”

5.6.1.7. Delitos globales

Los delitos globales, definidos por el Maestro Suñe, constituyen un fenómeno de nuevo cuño, vinculado a conductas antisociales de alcance y efectos directamente universales, por cuanto que se realizan a través de las grandes redes de transmisión de datos -hoy singularmente a través de Internet-. Se trata de delitos tales como la difusión de pornografía infantil, o la incitación a la violencia y al odio racial, en los cuales lo de menos es en qué país radique el servidor -ordenador- desde el que se difunden tales contenidos ignominiosos y lo demás es que su difusión alcanza a la vez a todos los países del orbe, lo que sin duda los diferencia de las formas tradicionales de delincuencia internacional, que nunca tuvo semejante grado de globalidad. (SUÑÉ LLINÁS, E., 2001)

El caso más práctico, por así decirlo, para explicar conceptualmente lo que los grandes doctrinantes han definido como delito global es el de la difusión de pornografía infantil, así lo cita el Doctor Suñé: *“Es más, el material política o sexualmente indecente, ni siquiera tiene por qué residir físicamente como tal material, en parte alguna, pues la tecnología informática posibilita que pueda estar segmentado en secuencias de bits radicadas en distintos servidores y países, que vistas aisladamente como tales secuencias en cada servidor o soporte singular, pueden no contener ni imágenes ni datos concretos, reuniéndose el contenido informacional, lingüístico o gráfico, sólo en destino; es decir en el ordenador del que accede a la información, sin que ello signifique -reitero- que tal información, al menos en forma asimilable por el ser humano, radique en forma comprensible, e incluso traducible para el mismo, en lugar alguno. O sea, que pensar que la competencia territorial para perseguir el delito, corresponde al Estado en el que radique determinado ordenador, es de una candidez de tal grado, que sólo es posible en base al usual desconocimiento, por parte de muchos juristas, de las insospechadas posibilidades que ofrecen la modernas tecnologías de la información y las comunicaciones. (SUÑÉ LLINÁS, E., 2001)”*

No podemos dejar de lado el componente técnico que reviste a los ciberdelitos o delitos universales, por ser cometidos estos con el uso de las nuevas tecnologías de la información y las comunicaciones, nos dice el maestro ibídem, que *“Los servidores desde los que se cometen los delitos globales, en el supuesto de que pueda identificarse el correspondiente material, suelen hallarse, además, en los denominados paraísos de datos, cuya erradicación -muy difícil por otra parte- ayudaría a combatir el fenómeno, igual que la desaparición de los paraísos fiscales, mantenidos con la complicidad y connivencia de los Estados y sobre todo de algunas grandes potencias,*

supondría un durísimo golpe contra la delincuencia internacional tradicional, al complicar sobremanera las operaciones de lavado de dinero.

El delito global se diferencia de la delincuencia internacional tradicional por su ubicuidad, lo que sin duda multiplica sus efectos, en aquellas cuestiones donde este delito es posible; pero también facilita su persecución, al no estar realmente delimitado por consideraciones de tipo territorial, pues no se trata realmente de un delito cometido en determinado Estado, sino que bien puede considerarse que se comete, a la vez, en los territorios de todos los Estados del orbe donde esté tipificado como tal delito, pues en todos ellos está accesible la correspondiente información” (SUÑÉ LLINÁS, E., 2001)⁷¹¹.

Ahora, para no enmarcarnos sin necesidad en delitos de pornografía, que para algunos Estados su tipificación es relativamente nueva, con el debido respeto, citamos nuevamente al maestro Suñé Llinás cuando enmarca como delito global el delito de incitación a la violencia o al odio racial, claramente en el esquema del Derecho Español, así:

“Cuando la incitación a la violencia o al odio racial se lleva a efecto a través de Internet u otras redes de transmisión de datos de carácter global, estamos ante un delito global, que por su propia naturaleza no puede entenderse cometido en el territorio de país alguno en concreto, sino en todos a la vez. Se trata, a fin de cuentas, de una situación abordable desde el artículo 23 de nuestra Ley Orgánica del Poder Judicial (LOPJ), relativo a la extensión y límites de la Jurisdicción española, pero

⁷¹¹ SUÑÉ LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

que rebasa con mucho los esquemas sociales, tecnológicos, e incluso mentales, de los que partió la redacción del mismo. Para eso está precisamente el denominado criterio sociológico de interpretación, que opera, en este caso, sobre una materia que no es de Derecho Penal sustantivo, sino orgánica y procesal de la Jurisdicción Penal. A mi juicio lo mejor es reproducir aquí el referido artículo 23 LOPJ, a fin de tener el punto de referencia concreto de nuestro propio sistema de Derecho positivo, a fin de proseguir el resto del estudio sobre la seguridad que dan las bases concretas, aun cuando no resulten del todo adecuadas:

- 1. En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte.*

- 2. Asimismo, conocerá de los hechos previstos en las leyes penales españolas como delitos, aunque hayan sido cometidos fuera del territorio nación al, siempre que los criminalmente responsables fueren españoles o extranjeros que hubieran adquirido la nacionalidad española con posterioridad a la comisión del hecho y concurrieren los siguientes requisitos:*
 - a) Que el hecho sea punible en el lugar de ejecución, salvo que, en virtud de un Tratado internacional o de un acto normativo de una Organización internacional de la que España sea parte, no resulte necesario dicho requisito⁷¹².*

⁷¹² El párrafo destacado en negrilla ha sido introducido por la Ley Orgánica 11/1999, de 11 de abril, de modificación del Título VIII, Libro II del Código Penal, en materia de delitos relativos a la libertad sexual, que corrigió -entre otros supuestos- el anterior vacío normativo existente en materia de pornografía infantil. Citado en: SUÑE LLINAS, E., 2001. El delito informático como

b) Que el agraviado o el Ministerio Fiscal denuncien o interpongan querrela ante los Tribunales españoles.

c) Que el delincuente no haya sido absuelto, indultado o penado en el extranjero, o, en este último caso, no haya cumplido la condena. Si sólo la hubiere cumplido en parte, se le tendrá en cuenta para rebajarle proporcionalmente la que le corresponda.

3. *Conocerá la jurisdicción española de los hechos cometidos por españoles o extranjeros fuera del territorio nacional cuando sean susceptibles de tipificarse, según la ley penal española, como algunos de los siguientes delitos:*

a) De traición y contra la paz o la independencia del Estado.

b) Contra el titular de la Corona, su Consorte, su Sucesor o el Regente.

c) Rebelión y sedición.

d) Falsificación de la firma o estampilla reales, del sello del Estado, de las firmas de los Ministros y de los sellos públicos u oficiales.

e) Falsificación de la moneda española y su expedición.

f) Cualquier otra falsificación que perjudique directamente al crédito o intereses del Estado, e introducción o expedición de lo falsificado.

g) Atentado contra autoridades o funcionarios públicos españoles.

h) Los perpetrados en el ejercicio de sus funciones por funcionarios públicos españoles residentes en el extranjero y los delitos contra la Administración Pública española.

i) Los relativos al control de cambios.

4. Igualmente será competente la jurisdicción española para conocer de los hechos cometidos por españoles o extranjeros fuera del territorio nacional susceptibles de tipificarse, según la ley penal española, como algunos de los siguientes delitos:

a) Genocidio.

b) Terrorismo.

c) Piratería y apoderamiento ilícito de aeronaves.

d) Falsificación de moneda extranjera.

*e) Los **delitos** relativos a la prostitución⁷¹³ y los de corrupción de menores o incapaces⁷¹⁴.*

f) Tráfico de ilegal de drogas psicotrópicas, tóxicas y estupefacientes.

⁷¹³ Entiendo que la expresión *esclavitud sexual*, debiera sustituir a la más usual de *delitos relativos a la prostitución*; puesto que la prostitución no es, ni debe ser delito, cuando afecta a personas mayores de edad que libremente la ejercen. Tampoco me parece correcta la vieja expresión *trata de blancas*, empleada incluso en antiguos Tratados Internacionales, como la Convención de París de 25 de julio de 1902, por tener connotaciones alusivas a una pretendida superioridad de la raza blanca. Existe asimismo un Convenio de represión de la trata de personas y explotación de la prostitución ajena, de 21 de marzo de 1950. Citado en: SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

⁷¹⁴ Lo señalado en negrilla fue asimismo introducido por la Ley Orgánica 11/1999, de 11 de abril, de modificación del Título VIII, Libro II del Código Penal, en materia de delitos relativos a la libertad sexual, con la finalidad -expresada en la exposición de motivos de la ley- de aplicar el principio de universalidad a la corrupción de menores e incapaces, *al responder unos y otros*- se refiere a los delitos relativos a la prostitución- *a la categoría internacional de delitos de explotación de seres humanos*. También se pone de manifiesto en la exposición de motivos, la no necesidad de doble incriminación, cuando resulte de un Tratado internacional, o de un acto normativo de una organización internacional de la que España sea parte. Citado en: SUÑE LLINAS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

g) Y cualquier otro que, según los tratados o convenios internacionales, deba ser perseguido en España.

En los supuestos de los apartados 3 y 4 será de aplicación lo dispuesto en la letra c) del apartado 2 de este artículo” (SUÑÉ LLINÁS, E., 2001)⁷¹⁵

5.6.1.8. La infracción de la regla *non bis in idem* como consecuencia de la actuación contra los delitos globales.

Una de las grandes preocupaciones de los Estados, al delegar la competencia funcional en un Tribunal Internacional para el juzgamiento de los ciberdelitos o delitos globales, es la posible infracción a la regla del *non bis in idem*.

Podría llegarse a pensar, que la persecución primaria de este tipo de delitos, por parte de un tribunal internacional, no sería excluyente de la competencia de los mismos Estados para hacerlo en búsqueda de alcanzar su *ius puniendi* estatal. Sin embargo la primera cualidad con la que se debe contar al momento del desarrollo de nuestra teoría, es precisamente que los Estados firmantes deben renunciar a su postestad de perseguir estas conductas denominadas y catalogadas previamente como ciberdelitos, para que sean perseguidas, investigadas, juzgadas y sancionadas únicamente por a través del mecanismo internacional.

Así lo ha planteado el maestro Suñé Llinás:

⁷¹⁵ SUÑÉ LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

“Un supuesto clásico de aplicación de la regla non bis in idem es el que se produce cuando un ciudadano del país A falsifica moneda del país B en el Estado C, con lo que ordinariamente infringirá leyes penales de los tres países. Algunos autores, como el ya citado Alcorta[29], defienden a capa y espada el axioma non bis in idem, pero no se debiera olvidar que la aplicación de este principio debe ceder ante supuestos de fraude de ley. De forma poco razonable, el propio Alcorta discute la opinión contraria, que pone en boca de Maurice Travers, según la cual si se admite la idea de que toda persecución en el extranjero, seguida de condena ejecutada o de absolución impidiese al delincuente ser llevado ante las jurisdicciones de otros Estados, los culpables podrían elegir hábilmente el lugar de represión y hacerse perseguir en el Estado que castigue con una pena menor al delito que han cometido. Probablemente tuviera una cierta razón Alcorta, cuando oponía a este argumento la rareza de la circunstancia -no olvidemos que su libro fue escrito en 1931-; pero esta pretendida rareza está destinada a no serlo tanto en el caso de los postcontemporáneos delitos globales, en los que los delincuentes tienen posibilidades tecnológicas a su alcance hace poco tiempo inimaginables, tales como situar impunemente los ordenadores que empleen en paraísos de datos, e incluso suministrar a la vez datos incompletos -incluso sin sentido, vistos aisladamente- desde varios países, que sólo serían incompletos en cada uno de ellos -y aun conjuntos ininteligibles de ceros y unos-y que sólo la acción del usuario de un ordenador-cliente, en cuanto a solicitarlos, reunificaría de forma completamente inteligible este material delictivo en el país donde estuviera el cliente. Las posibilidades de fraude de ley son ahora enormes y, por ello, hay que darle la misma importancia que a la propia regla non bis in idem. (SUÑÉ LLINÁS, E., 2001)

Algunas pistas sobre cómo perseguir los delitos globales, que en el fondo abonan las tesis aquí mantenidas, se dan en el caso de los delitos a distancia, como en el supuesto del envío de un paquete bomba desde el país A, que produce una muerte en el Estado B; delitos que -no lo olvidemos-, se producen también en materia de virus y sabotajes informáticos. La legislación y la doctrina se ha mostrado dividida entre las teorías de la acción y del resultado, en cuanto al país que resulta competente para enjuiciar y penar este tipo de acciones; pero últimamente se abre paso la teoría de la ubicuidad, brillantemente defendida entre nosotros por Muñoz Conde y García Arán, por ejemplo cuando dicen:

Si “matar” significa realizar una conducta dirigida a producir un resultado de muerte que termina produciéndolo, el hecho de “matar” no se comete exclusivamente ni en el momento de la acción ni en el momento de la producción de la muerte, sino en ambos; ello coincide, evidentemente, con la tesis de la ubicuidad⁷¹⁶.

En principio, el país donde está el autor de los hechos, es el que más fácil tiene juzgarle y condenarle; pero nada obsta a que se pida la extradición. Esta construcción de la ubicuidad que diluye la estricta territorialidad del Derecho Penal, es perfectamente aplicable al delito global, incluido lo relativo a las facilidades para juzgar al autor del crimen o la posible petición de extradición. (SUÑÉ LLINÁS, E., 2001)

Cierto es que este tipo de solución debiera entenderse como provisional, hasta tanto se aprobase un Tratado Internacional relativo a los delitos globales, que sería lo deseable, e incluso lo ideal sería que dicho Tratado

⁷¹⁶ F. Muñoz Conde y M. García Arán, op. cit. Pág. 171. SUÑÉ LLINÁS, E., 2001. El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Alfa Redi: Madrid.

estableciese una tipificación uniforme de los mismos, al menos en la medida en que se fuesen detectando, y una competencia judicial basada en lo posible en el principio de efectividad, sin que ni siquiera sea imprescindible la creación de un órgano jurisdiccional internacional. (SUÑÉ LLINÁS, E., 2001)

5.6.1.9. Principio de Justicia Universal.

Un elemento primordial de los planteamientos desarrollados en este trabajo investigativo consiste en estructurar la justicia con carácter universal, que es la que permite la persecución de delitos, en primera instancia por órganos internacionales.

El principio de justicia universal ha sido desarrollado por los autores españoles Jiménez y García en su obra el Principio de Justicia Universal, fundamentos y límites, cuando establecen:

“Desde esta perspectiva, defendemos la postura que han adoptado algunos tribunales a la hora de aplicar el principio de justicia universal. En este sentido, se ha manifestado nuestro Tribunal Constitucional en la Sentencia 237/2005, de 26 de septiembre, sobre el asunto de Guatemala que vuelve a proclamar el carácter absoluto y pleno del principio de justicia universal declarado en el artículo 23.4 LOPJ, haciéndose eco de la misma inmediatamente la comunidad jurídico-internacional. De esta relevante decisión hemos de destacar los siguientes elementos concordantes con la práctica internacional anteriormente mencionada. (JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012: 193)

i) En primer lugar, la precisión acerca del carácter concurrente que tiene el principio de justicia universal respecto a otros títulos competenciales, en particular, el principio de territorialidad. A tal efecto se reproduce el dictum de la Sentencia 87/2000 anteriormente citado, precisándose que «resulta indudable que existen razones de peso, tanto procesales como político-criminales, que vienen a avalar la prioridad del locus delicti, y que ello forma parte del acervo clásico del Derecho internacional penal. Partiendo de este dato, y retomando la cuestión que dejamos pendiente, lo cierto es que, desde el plano de su formulación teórica, el principio de subsidiariedad no habría de entenderse como una regla opuesta o divergente con la que introduce el llamado principio de concurrencia, y ello porque, ante la concurrencia de jurisdicciones, y en aras de evitar una eventual duplicidad de procesos y la vulneración de la interdicción del principio ne bis in ídem, resulta imprescindible la introducción de alguna regla de prioridad. Siendo compromiso común (al menos en el plano de los principios) de todos los Estados la persecución de tan atroces crímenes por afectar a la comunidad internacional, una elemental razonabilidad procesal y político-criminal ha de otorgar prioridad a la jurisdicción del Estado donde el delito fue cometido». (JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012: 193)⁷¹⁷

Dentro de esta razonabilidad jurídica y procesal se afirma que para la activación de la jurisdicción universal extraterritorial «habría de ser,

⁷¹⁷ JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012. Propuesta de Convención universal sobre el principio de justicia universal: algunas reflexiones. En: PÉREZ CEPEDA, A. I. (Eds). EL PRINCIPIO DE JUSTICIA UNIVERSAL: Fundamentos y límites. Tirant lo Blanch: Valencia. P. 193

entonces, suficiente con que se aportaran, de oficio o por la parte adora, indicios serios y razonables de la inactividad judicial que vinieran a acreditar una falta, ya de voluntad, ya de capacidad para la persecución efectiva de los crímenes» por parte del Estado territorial. (JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012: 194).

Sin embargo, para el desarrollo de nuestra tesis este principio de universalidad extraterritorial no debe contemplar la inactividad de los Estados en su aspecto territorial, al contrario, los Estados deben permanecer activos en la persecución penal de los ciberdelitos, para que de esta forma cuando conozcan de la comisión de conductas que eventualmente puedan configurarse como ciberdelitos sean respetuosos con las competencias funcionales que ejercería el Estatuto de Roma a través de la Corte Penal Internacional dentro de la tesis que desarrollamos.

Continúan los autores en cita, definiendo:

“A efectos de concurrencia de jurisdicciones, resultan oportunos los criterios de complementariedad positivados en el Estatuto de Roma cuando afirma su competencia a pesar de que en el Estado territorial se han llevado a cabo actuaciones tendentes a enjuiciar o sancionar al sujeto en cuestión. Al respecto debemos citar el artículo 17 del Estatuto de Roma, y siguiendo tales criterios, se debe afirmar la competencia universal cuando el Estado territorial o el de la nacionalidad del sujeto acusado no lo juzgan porque no quieren o porque no tienen capacidad para ello, o cuando habiendo entablado una persecución hay indicios de que dicha persecución es fraudulenta, esto es, con la finalidad de sustraer a los sujetos acusados de la justicia penal de otros Estados o de una Corte Penal Internacional, y cuando no se han respetado los derechos fundamentales ni las garantías procesales exigidas por el

Derecho internacional de los derechos humanos. (JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012: 194)

Estos criterios que determinan cuando el principio de justicia universal puede afirmarse debido a su carácter subsidiario o complementario ya han sido establecidos por la práctica jurisprudencia nacional y por algunas legislaciones. Tales son el asunto Cvjetkovic en Austria o la Ley de Croacia de 2003, y por supuesto en la doctrina constitucional española reseñada. También la Corte Interamericana de Derechos Humanos (en adelante Corte IDH) y los tribunales internacionales ad hoc (como marcan sus Estatutos respectivos), han venido a delimitar el funcionamiento del principio de justicia universal como subsidiario al de territorialidad en el sentido expuesto. Así en el Caso Almonacid Arellano y otros, sentencia de 26 de septiembre de 2006, la Corte IDH ha determinado que con relación al principio ne bis in ídem, los tribunales nacionales podrán volver a juzgar a sospechosos en aquellos casos en los que el primer juicio haya tenido por objeto sustraer al sujeto de la justicia o no se haya llevado con independencia o imparcialidad. (JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012: 194)⁷¹⁸

Vemos entonces que la actuación de los Estados en la búsqueda de la justicia universal y en la búsqueda de protección de los derechos humanos fundamentales e inherentes al ser no puede materializarse a través de la ignorancia, inoperatividad e inactividad frente a la persecución de conductas eventualmente lesivas a bienes jurídicos tutelados, por el contrario debe permanecer atento a su persecución e identificación y en el momento en el

⁷¹⁸ JIMÉNEZ GARCÍA, F., GARCÍA SÁNCHEZ, B. 2012. Propuesta de Convención universal sobre el principio de justicia universal: algunas reflexiones. En: PÉREZ CEPEDA, A. I. (Eds). EL PRINCIPIO DE JUSTICIA UNIVERSAL: Fundamentos y límites. Tirant lo Blanch: Valencia. P. 194

que se cumplan los criterios y características que definen los ciberdelitos debe remitir su conocimiento al que sería el órgano competente, es decir, la Corte Penal Internacional, sin que esto signifique que el Estado renuncia al ejercicio de su *ius Puniendi*, por el contrario, lo ha materializado en la competencia que entregó a la Corte internacional.

6. CONCLUSIONES

Mariela Machado, en el año 2009 publica en línea un artículo denominado Definición de una frontera clara entre la jurisdicción nacional y la proclamada del Tribunal Penal Internacional. En este estudio se plantean los principales interrogantes a los que hemos dado respuesta en el desarrollo de esta Tesis Doctoral, debemos de esta forma empezar por establecer que el mundo globalizado ha cerrado las brechas territoriales entre los Estados y ha traspasado las fronteras entre los pueblos.

La globalización como fenómeno ha generado en el mundo avances más que significativos dentro del desarrollo político, económico y social de las naciones. La principal representación material del mundo globalizado se ha dado a través de los medios de comunicación, que desde finales del siglo XX fueron revolucionados por nuevas herramientas como INTERNET, donde a través de una red global o maestra ha sido posible compartir información y datos entre sujetos, cualquiera que sea su categorización, a velocidades antes inimaginables.

Es entonces esta transferencia de datos y de información entre los sujetos a través de Internet como representante de las Tecnologías de la Información y las comunicaciones la que en todo el desarrollo argumentativo realizado, busca ser objeto de protección.

Por esa razón hemos realizado un recuento de las principales legislaciones europeas, la canadiense y la estadounidense donde mostramos los ámbitos de protección y los mecanismos legales establecidos para ello.

No obstante lo anterior, nos hemos centrado en un recuento específico de la legislación frente a delitos informáticos en los Estados de Colombia y España, demostrando cual ha sido su desarrollo histórico, su creación legal y su análisis desde la dogmática penal. Lo que nos enseña la importancia de la protección desde el ámbito constitucional y su trasposición al derecho de última ratio, dándole protección desde el ámbito penal, creando mecanismos que permiten su persecución desde la investigación hasta el juzgamiento y sanción.

Tenemos entonces como antecedente que los Estados en ejercicio de su autonomía y soberanía han decidido perseguir penalmente a quienes ejecutan conductas que se tipifican como delitos informáticos o delitos en contra de la información y los datos como bienes jurídicos tutelados. Sin embargo, al igual que en la persecución y sanción de cualquier otra categoría de delito, las fronteras creadas no solo por el territorio sino por el concepto de jurisdicción y competencia que son los delimitantes del ejercicio punitivo de los Estados, impiden que se investigue, juzgue y sancione a un sujeto que ha cometido la conducta desde un territorio pero con consecuencias en otro, o por el contrario la cometió desde un Estado pero las víctimas o el daño se materializan en otro, teniendo en cuenta este concepto, no podrá ni debe haber fronteras en la búsqueda de terminar la impunidad en los delitos informáticos.

Es de esta forma que el planteamiento anterior nos lleva a determinar la necesidad de buscar un sistema de justicia universal que permita la investigación juzgamiento y sanción de los delitos informáticos o delitos que atentan contra la información y los datos. Es en este sentido que hemos concluido que la mejor forma para lograrlo es que los Estados de forma voluntaria renuncien a esta categoría de su *Ius Puniendi*, de forma que la

persecución de esta clase de delitos, para cada Estado, no sea de tipo principal, sino que esta función recaiga de manera primaria sobre una organización internacional.

Después del respectivo análisis doctrinal y jurisprudencial correspondiente hemos definido que el Organismo Internacional más adecuado, sobre el cual debe recaer la función punitiva frente a los delitos informáticos es la Corte Penal Internacional, debido a sus características y sistema organizacional que permiten a través de la forma de adhesión voluntaria de los Estados, que sea esta quien asuma la investigación, juzgamiento y sanción de estas conductas.

La anterior conclusión tiene como sustento el precepto según el cual los derechos humanos son universales y que esta categoría no puede depender de las condiciones políticas, sociales y económicas de los Estados, por el contrario, deben ser garantizados pues hace parte de la deontología de cada Estado protector.

Bajo esta concepción es evidente que el derecho a la justicia, debe ser tanto de carácter humano, como universal, lo que nos lleva a establecer el principio de justicia universal, que solo es posible configurar cuando los Estados, como se dijo anteriormente renuncian al *ius Puniendi* de manera primaria, para dejarlo en manos de la Corte Penal Internacional como Organización Internacional en los casos en los que los delitos son también universales, como se ha podido establecer tras la caracterización de los delitos informáticos.

No olvidemos entonces para lograr el objetivo anteriormente estipulado, la conceptualización realizada por SUÑÉ LLINÁS, cuando establece que:

“No hay que perder de vista, especialmente, la advertencia de Wolff, según la cual, si bien hay que clamar por el principio de universalidad del Derecho Penal, ante las violaciones más graves del Derecho Natural, no por ello se debe eliminar su vinculación ordinaria a la soberanía del Estado. Algunos siglos después, pienso más o menos lo mismo, por muchas razones, entre ellas que el principio de territorialidad del Derecho Penal es una prerrogativa del Estado, pero también una garantía para los ciudadanos de todo el orbe, pues si los Estados ejercieran ordinariamente su potestad para establecer y perseguir delitos más allá de las propias fronteras, todos tendríamos la inquietud de poder vernos sometidos, en cualquier momento y por las circunstancias más variopintas, a la potestas puniendi de cualquier Estado, como le sucedió a Rushdie con la fatwa de Jomeini” . (SUÑÉ LLINÁS, E., 2001)

Retomando los planteamientos del doctor Suñe Llinas, podemos concluir que avocando el principio universal del derecho penal, es necesario brindar la protección jurídica a bienes tutelados nacientes de las nuevas formas sociales, económicas y tecnológicas a través de un órgano de carácter universal, para el que, en este caso concreto, consideramos que la competencia debe recaer en la Corte Penal Internacional, de forma que dicha regulación de la tranquilidad jurídica a las víctimas de los delitos informáticos, quienes tienen la seguridad tanto emocional como jurídica, de que la violación a sus derechos no será impune, y que al mismo tiempo tenga el velo de protección emanado de los principios generales del derecho, según el cual la política criminal universal no perseguirá internacionalmente delitos que se mantengan dentro de la órbita territorial de cada estado y que se definan en el ámbito de protección personal de cada lus Puniendi estatal. Así mismo, Kai

Ambos, ha establecido que El motivo de interés de los ataques informáticos es que por lo general solo estas formas de delitos cometidos en el ciberespacio son lo suficientemente serias para ser calificadas como crímenes internacionales, y así quedar cubiertas por una jurisdicción penal internacional. (AMBOS, K. 2014:13)⁷¹⁹

Sin embargo, una de las principales características del Estatuto de Roma, documento guía del funcionamiento de la Corte Penal Internacional, como se dijo anteriormente, es el carácter subsidiario del Estatuto para el juzgamiento de conductas penales ante la Corte Penal Internacional, entonces nuestro desarrollo investigativo nos ha llevado a concluir que la solución a corto plazo consiste en la aplicación de la teoría del delito UBICUO o global planteada por el Maestro Suñé Llinás, donde los Estados, haciendo uso del principio de interpretación extensiva del derecho penal, y como requisito previo, teniendo una legislación que tipifique los delitos informáticos, electrónicos o de las telecomunicaciones ya sea por su naturaleza o por el mecanismo de comisión. Esto teniendo en cuenta y siendo claros en el tiempo que implica para los Estados la celebración de una modificación a un tratado internacional, que constituye la solución a largo plazo para la investigación, juzgamiento y sanción de los ciberdelitos.

Retomando entonces, la verdadera solución a largo plazo consistiría como punto de partida la modificación al Estatuto de Roma, donde los ciberdelitos o delitos universales no sean conocidos por la Corte Penal Internacional de forma subsidiaria o residual, sino que, por el contrario, por tratarse de delitos Universales, es esta instancia de Derecho Penal Internacional quien cuenta con los requisitos y calidades para adelantar su persecución, siendo este órgano quien realice su investigación, juzgamiento y sanción, desde que se

⁷¹⁹ AMBOS, K. (2014) Responsabilidad Penal Internacional en el ciberespacio. Bogotá D.C.: Centro de Investigación en Filosofía y Derecho. Universidad Externado de Colombia.

tenga conocimiento de su comisión, como instancia primaria, nunca subsidiaria, donde el objetivo claro es la aplicación del *Ius Puniendi*, ya no Estatal, sino Universal.

Además se hace indispensable que los Estados que se constituyan como partes para la investigación, juzgamiento y sanción de los ciberdelitos, acuerden en una instancia inicial la tipificación de una serie de delitos como ciberdelitos, globales o universales, revistiéndolos de las características técnicas que permiten identificar cuando su comisión ha surgido a través del ciberespacio y de esta forma sobrepasa las barreras del territorio.

Dentro de los principales componentes de este Tratado de Internacional del Ciberespacio, como hemos decidido denominarlo, debe concentrarse la lucha contra la impunidad de los delitos globales o transversales en el mundo, cuyo objetivo sea el mantenimiento de la seguridad jurídica de los seres humanos, tomando como punto de partida los Principios generales del Derecho Penal y creando circunstancias comunes a las atribuciones del *Ius Puniendi* de cada uno de los miembros, lo anterior so pena de que implique modificaciones dentro de la política criminal de los Estados que se hagan miembros y dentro de sus sistemas penales, de forma que la competencia territorial no se convierta en un obstáculo para que los seres humanos sean merecedores de la justicia, al contrario, que al dejar de lado el concepto anterior de territorialidad legislativa se otorgue a las víctimas (individuales o colectivas) la reivindicación de sus derechos vulnerados y de los bienes jurídicos (de nuevo individuales o colectivos) que hayan podido ser menoscabados.

IV. BIBLIOGRAFÍA

- AMBOS, K. (2006). La parte general del Derecho Penal Internacional. Bogotá D.C.: Editorial Temis.
- AMBOS, K. (2014) Responsabilidad Penal Internacional en el ciberespacio. Bogotá D.C.: Centro de Investigación en Filosofía y Derecho. Universidad Externado de Colombia.
- BAÓN RAMÍREZ, R. (1996) "*Visión general de la informática en el nuevo Código Penal*", en *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, Madrid: Escuela Judicial/Consejo General del Poder Judicial
- BARREIROS, L.E., LAVOPA, F., PINTO, M., RICART, L.T., TURYN, A. (2009). Las fuentes del Derecho Internacional en la Era de la globalización. Buenos Aires: Editorial Universitaria de Buenos Aires. Primera Edición.
- BARRIUSO RUIZ, Carlos. 1996. "Interacción del Derecho y la informática", Madrid: Dykinson.
- BAUMAN, Z. (2003). *Modernidad Líquida*. Buenos Aires: Fondo de Cultura Económica.
- BBC Mundo/Economía, Microsoft contra el "cibercrimen", miércoles, 5 de noviembre de 2003, http://news.bbc.co.uk/hi/spanish/business/newsid_3245000/3245243.stm, página visitada en abril de 2007.
- BECK, U. (2002). *La Sociedad del Riesgo global*. Madrid: Sigo XXI Editores
- BLÁSQUEZ PEINADO, M.D. 2003 La Corte Penal Internacional y su aportación a la teoría general de las organizaciones internacionales. En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL

INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach

- BROTONS, A.R., CORTADO RIQUELME, R., DIEZ-HOCHLEITNER, J., ORIHUELA CALATAYUD, E., PÉREZ-PRAT DURBÁN, LUIS. (2007). Derecho Internacional. Valencia: Tirant Lo Blanch.
- BUSTOS, J., HOMAZÁBAL, H. (2006). Lecciones de Derecho Penal Parte General. Madrid: Trotta
- CAMPOLI, G.A. (2002) "Hacia una correcta Hermenutica Penal - Delitos Informáticos vs. Delitos Electrónicos", No. 048 - Julio del 2002, AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi. <http://www.alfa-redi.org/rdi-articulo.shtml?x=1480>, Página consultada marzo de 2007
- CARDONA LLORÉNS, J. (2003). La Corte Penal Internacional y el mantenimiento de la paz y la seguridad Internacionales, en: En: GÓMEZ COLOMER, J.L. (Eds). LA CORTE PENAL INTERNACIONAL UN ESTUDIO INTERDISCIPLINAR. Valencia España.: Editorial Tirant lo blach.
- CASTELLS, Manueol. (2006a). *La era de la información. Economía, sociedad y cultura. La sociedad red. Vol. I.* México: Siglo XXI Editores, 7ª ed.
- CASTRO ARGÜELLO, M. J., TOBARES CATALÁ, G. H., (2006) Delitos Informáticos. Córdoba, Argentina: Editorial Advocatus.
- CASTRO CUENCA, C., HENAO CARDONA, L., BALMACEDA HOYOS, G., 2009. Derecho Penal en la sociedad del riesgo. Bogotá D.C.: Grupo Editorial Ibañez.
- CHEHTMAN, A. (2013). Fundamentación filosófica de la justicia penal extraterritorial. Marcial Pons: Madrid.
- CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional)

<http://www.uncitral.org/pdf/spanish/texts/payments/guarantees/guarantees-s.pdf>, página consultada Febrero de 2008.

- COHEN, D. (2007). *Tres lecciones sobre la sociedad postindustrial*. Buenos Aires: Katz Editores
- CUERVO, J. (1999), "Delitos informáticos: protección penal de la intimidad", AR: Revista de Derecho Informático, ISSN 1681-5726, Edita: Alfa-Redi, No. 006 – Enero del 1999., <http://www.alfa-redi.org/rdi-articulo.shtml?x=207> página web consultada abril 2007.
- DAVARA RODRÍGUEZ, M. A. (1997) *"Manual de Derecho Informático"*, Pamplona: Editorial Aranzadi.
- De la MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L. (2010) *Derecho Penal Informático*. Pamplona, España: Editorial Thomson Reuters. Civitas
- DÍAZ GARCÍA, A., RINCÓN RÍOS, J., (2009). Trámite y exposición de motivos Ley 1273 de 2009. Bogotá D.C. Colombia: Editorial Universidad Santiago de Cali.
- FALCÓN y TELLA, F., (2004). Para una Teoría del Conocimiento. *Foro, Nueva época*, núm. 00/2004: 69-89.
- Fiscal General de la Nación en Colombia, en concepto rendido dentro de la sentencia constitucional C-739 de Junio 22 de 2000. en donde se habla del principio de legalidad. Magistrado Ponente Dr. Fabio Morón Díaz. <http://www.corteconstitucional.gov.co/relatoria/2000/c-739-00.htm>; página consultada Febrero de 2007
- FOUCAULT, M. (1966). *Las palabras y las cosas*. Madrid: Siglo XXI Editores.
- FOUCAULT, M. (1976). *Vigilar y Castigar. Nacimiento de la prisión*. Buenos Aires: Siglo XXI editores,
- GIDDENS, A. (1992). *The consequences of Modernity*. Cambridge: Polity Press.

- HARDT M. y NEGRI. A. (2002). *Imperio*. Buenos Aires: Paidós. 1ª edición compactada
- Instituto Nacional de Tecnologías de la comunicación de España. Pagina Oficial <http://www.inteco.es> Informe de adecuación de la Ley de a la Ley de servicios de la Sociedad de la información y de comercio electrónico. De diciembre de 2012. Tomado desde: https://www.incibe.es/file/oqQycDyL33mC_bcRKSfBg el 10 de enero de 2015.
- IRIARTE AHON, E. (2005) “Sociedad de la información: Políticas y Regulación en América Latina y el Caribe ¿Hacia dónde vamos los profesionales del derecho y las nuevas tecnologías?”, AR: Revista Derecho Informático, ISSN 1681-5726, Ed. Alfa Redi, No. 089, Diciembre de 2005, página consultada febrero 2007.
- JOVER PADRÓ, Josep. 1997. *"El Código Penal de la informática"*, X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Pamplona: Aranzadi Editorial
- LÉVY, P. (1999). *¿Qué es lo virtual?* Barcelona: Paidós Multimedia.
- LIPOVETSKY, G. (2000). *La era del vacío. Ensayos sobre el individualismo contemporáneo*. Barcelona: Anagrama
- LÓPEZ ZAMORA, P. (2006), en TRATADO DE DERECHO INFORMÁTICO VOLUMEN II. Coordinador SUÑE LLINAS, E. (2006) Madrid: Universidad Complutense de Madrid
- MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogota D.C.: Leyer,
- MÁRQUEZ ESCOBAR, P.C. (2002). *El delito Informático*. Bogotá, Colombia: Leyer.
- MARX, K. (2002). México: Siglo XXI Editores. *El Capital*
- MÖHRENSCHLAGER, M. E., “Computer crimes and other crimes against information technology in Germany” en “Information

Technology crime. National legislation and international initiatives”. Berlín Bonn, Manchen: Ed. Sieber, U., Köln.

- MUÑOZ CUESTA, F. J. (2009). Estafa informática, introducción de datos falsos en operaciones mercantiles vía internet que motivan transferencias de dinero no consentidas. Revista Arazandi Doctrinal Num. 1/2009. Tomado desde: [http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishing/Article.%20Estafa%20inform%E0tica%20\(mo%20lt%20bo\).pdf](http://cv.uoc.edu/~g092_03_504_02_08_w01/PAC2/articles%20juridics%20sobre%20phishing/Article.%20Estafa%20inform%E0tica%20(mo%20lt%20bo).pdf) el 20 de enero de 2013.
- NARANJO DUQUE, V., RINCÓN RÍOS, J. (2011). Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia. Cali, Colombia: Editorial Universidad Santiago de Cali.
- NUÑEZ, P.T., (2009). Los Tribunales españoles y las decisiones de los órganos convencionales de Derechos Humanos en el ámbito universal. ¿Condenados a defenderse? En: Tribunales Internacionales y espacio Iberoamericano. Civitas. Madrid, España.
- ORTEGA JIMÉNEZ, A. (2003). “La regulación de internet”, Revista electrónica alfa-Redi, No. 061, agosto 2003, <http://www.alfa-redi.org/rdi-articulo.shtml?x=9464>, ISSN, 1681-5726, página consultada marzo de 2007.
- PABÓN PARRA, P.A., (2002). Manual de Derecho Penal Parte general – Parte especial. 6ª Bogotá D.C.: Edición. Doctrina y Ley Ltda.
- PALOMINO MARTIN, J.M., (2006). Derecho Penal y Nuevas Tecnologías. Hacia un sistema informático para la aplicación del Derecho Penal. Valencia, España: Tirant lo Blanch.
- PEÑA VALENZUELA, D., (2007). Responsabilidad civil en la era digital. Bogotá D.C. Colombia: Editorial Universidad Externado de Colombia.
- PÉREZ CEPEDA, A. I. (Eds). EL PRINCIPIO DE JUSTICIA UNIVERSAL: Fundamentos y límites. Valencia: Tirant lo Blanch:

- Portela Calderón, Carlos y Díaz Héctor, “Delitos Informáticos”, Universidad Cooperativa de Colombia, Facultad de Derecho, 2004. p. 6, www.alediag@net.com
- REY CANTOR, E. (2006), “Las generaciones de los derechos humanos”, Bogotá D.C.: Universidad Libre, cuarta edición, ISBN 958-676-346-1
- REYES, A. (1972), “Derecho Penal, Parte General”, 2da edición, Publicaciones Universidad Externado de Colombia, Bogotá.
- REYNA ALFARO, L. M., (2002) Los Delitos Informáticos. Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima: Juristas Editores.
- RINCÓN CÁRDENAS, E. (Eds) 2006. Contratación Electrónica, Bogotá D.C.: Centro Editorial Universidad del Rosario.
- RINCÓN RÍOS, J. (2010). Ponencia presentada en el XIV CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA en la UNIVERSIDAD AUTONOMA DE NUEVO LEON – MONTERREY - MEXICO en fecha OCTUBRE 25 AL 30 DE 2010.
- RINCÓN RÍOS, J. (2011). Justicia Internacional, una alternativa válida para el Delito Electrónico. Ponencia presentada en el Foro Delito Informático En Colombia, (Evaluación necesaria a dos años de inicio). Seguridad Informática Vs Delito Febrero 23 al 25 de 2011. Ponencia presentada en la Universidad Santiago de Cali. Cali, Colombia.
- RINCÓN RÍOS, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.
- RINCÓN RÍOS, J. y NARANJO DUQUE, V. (2013). *Delito informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia*. Bogotá: Grupo Editorial Ibáñez.
- RODRÍGUEZ AZUERO, S. (2006) Referencias a la contratación bancaria electrónica en Colombia, aparece en obra colectiva

Contratación Electrónica, en: Erick Rincón Cárdenas (Eds) Bogotá D.C.: Centro Editorial Universidad del Rosario.

- RODRÍGUEZ BARRIGÓN, J. M. (2006). Tribunales Penales Internacionalizados: La especialización de la Justicia Penal. En: Carlos R. Fernández Liesa (Eds.) Tribunales Internacionales y espacio Iberoamericano. Tomson civitas: Madrid.
- ROMEO CASABONA, C. M. (1996). *"Delitos informáticos de carácter patrimonial"*, Informática y Derecho nº 9,10 y 11. Mérida: UNED, Centro Regional de Extremadura.
- ROVIRA del CANTO, E. (2002) Delincuencia Informática y fraudes informáticos. Granada: Editorial Comares.
- RUSCONI, M., (2009). Derecho Penal Parte General., Buenos Aires: 2ª edición. AD-HOC. SUÑÉ LLINÁS, E. (2009) Filosofía jurídica y política de la nueva ilustración. Estudios en homenaje a la Escuela Libre de Derecho en su primer centenario. México D.F.: Porrúa.
- SUÑÉ LLINÁS, E. (2009) Filosofía jurídica y política de la nueva ilustración. Estudios en homenaje a la Escuela Libre de Derecho en su primer centenario. México D.F.: Porrúa.
- SUÑE LLINAS, E., (2001). El delito informático como motor de cambios conceptuales en el Derecho Penal. En Revista de Derecho Informático ISSN 1681-5726 No. 40 de noviembre de 2001. Madrid: Alfa Redi.
- SUÑE, LLINAS. E., (2009). *Los Derechos Humanos en el Ciberespacio. La Declaración de derechos del Ciberespacio*. Madrid: ACTAS DE LA II CONVENCIÓN INTERNACIONAL DE DERECHO INFORMÁTICO.
- TELLEZ VALDÉS, Julio. 1996. *"Los Delitos informáticos. Situación en México"*, Informática y Derecho nº 9, 10 y 11, Mérida: UNED, Centro Regional de Extremadura
- Touraine, Alain. (1994). *Crítica de la modernidad*. México: Fondo de Cultura Económica

- TOURAINE, Alain. (2000). *¿Podremos vivir juntos?* Bogotá: Fondo de Cultura Económica
- UNESCO. (1972). *Informe Faure. Aprender a aprender*. Paris: Unesco
- UNESCO. (2005). *Hacia la sociedad del Conocimiento*. Paris: Unesco.
- VELÁSQUEZ VELÁSQUEZ F., (2010). *Manual de Derecho Penal*. Bogotá D.C.: Cuarta Edición, Ediciones Jurídicas Andrés Morales.
- VIRILIO, P. (1998). *La bomba informática*. Paris: Galilée
- ZAFFARONI, E. R., ALAGIA, A., SLOKAR, A. (2002). *Derecho Penal Parte General*. Buenos Aires: EDIAR.

V. CIBERGRAFÍA

- Acuerdo de relación entre la Corte Penal Internacional y las Naciones Unidas. Extraído el 24 de mayo de 2005, desde: http://www.icc-cpi.int/NR/rdonlyres/3EBEECA5-0EAC-4685-950F-1488CF56BE64/0/ICCASP3Res1_Spanish.pdf
- Acuerdo sede entre la Corte Penal Internacional y los Estados partes. Extraído el 24 de mayo de 2011, desde: <http://www.icc-cpi.int/NR/rdonlyres/99A82721-ED93-4088-B84D-7B8ADA4DD062/280775/ICCBD040108ENG1.pdf>
- Acuerdo sobre los Privilegios e Inmunidades de La Corte Penal Internacional. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/23F24FDC-E9C2-4C43-BE19-A19F5DDE8882/140093/APIC_Spanish.pdf
- CARNELUTTI, Francesco. Cómo nace el derecho. Traducción de Santiago Sentís Melendo y Marino Ayerra Redín. Colección Monografías Jurídicas. Editorial Temis, Segunda Edición, Santa Fé de Bogotá, 1994. Citado en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>
- CARNELUTTI, Francisco. Teoría General del Derecho. Traducción de Francisco J. Osset. Editorial Revista de Derecho Privado, Madrid, 1955. Citado en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>
- CASTRO OSPINA, S.J., (2008, febrero). Algunos Aspectos Dogmáticos De La Delincuencia Informática. Extraído el 26 de marzo de 2011, desde: <http://www.delitosinformaticos.com/02/2008/delitos/algunos-aspectos-dogmaticos-de-la-delincuencia-informatica>

- CHACMN, I. (1925, diciembre 1925). Revista "ASTREA", de Derecho y Legislación en Ciudad Bolívar, Tomo 1, N ° 12. Extraído el 5 de abril de 2011. Página. 240 desde: <http://acienpol.msinfo.info/bases/biblo/texto/L-714/A-12.pdf>
- Código de conducta profesional de los abogados. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/BD397ECF-8CA8-44EF-92C6-AB4BEBD55BE2/140124/ICCAPSP4Res1_Spanish.pdf
- Código de ética judicial. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/A62EBC0F-D534-438F-A128-D3AC4CFDD644/140141/ICCBD020105_En.pdf
- CORREA, M., MORA, N., Noguera, E., Parra, I., Sierra, I., (2005, Marzo 18). Extraído el 29 de marzo de 2011. Desde: <http://www.monografias.com/trabajos17/delitos-electronicos/delitos-electronicos.shtml>.
- CRESTO, A.E., (2010, octubre 29). La pornografía infantil en el marco de los delitos informáticos y del llamado “derecho penal de las sociedades de riesgo”. Cuestiones problemáticas. Extraído el 26 de marzo de 2011, desde: http://www.jovenespenalistas.com.ar/Pornografia_infantil_Crespo_Alv_aro.pdf
- Elements of Crimes. Extraído el 24 de mayo de 2011, desde: <http://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf>
- FALCON y TELLA, F. (2004, diciembre). Valores, Normas y Hechos y en el Derecho. Extraído el 4 de abril de 2011. Desde: http://www.cepc.es/rap/Publicaciones/Revistas/3/REPNE_126_323.pdf
- KANT, Manuel. Principios metafísicos de la doctrina del derecho. Editorial Universidad Autónoma de México, México D.F., 1968. Citado

en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>

- LÓPEZ WONG, R.S., (2003, mayo). ACERCA DE LA DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS. DETERMINACIÓN DE LA NATURALEZA JURÍDICA DE LAS CONSECUENCIAS ACCESORIAS: ¿SANCIÓN PENAL O MEDIDA ADMINISTRATIVA? Extraído el 26 de marzo de 2011, desde: http://www.urbeetius.org/newsletters/06/news6_lopezwong.pdf
- MACHADO, M. (marzo 29 de 2011). Extraído el 26 de marzo de 2011, desde: <http://www.terragnijurista.com.ar/doctrina/responsabilidad2.htm>.
- PACHECO, Máximo. Teoría del Derecho. Editorial Temis S.A., cuarta edición, Santa Fé de Bogotá, 1990, pág. 739. Citado en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>
- Reglamento de la Corte Penal Internacional. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/B920AD62-DF49-4010-8907-E0D8CC61EBA4/277531/ICCBD010104_Spanish.pdf
- Reglamento de la Oficina del Fiscal. Extraído el 24 de mayo de 2011, desde: <http://www.icc-cpi.int/NR/rdonlyres/FFF97111-ECD6-40B5-9CDA-792BCBE1E695/280253/ICCBD050109ENG.pdf>
- Reglamento de la Secretaria. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/A57F6A7F-4C20-4C11-A61F-759338A3B5D4/140152/ICCBD_030106_Spanish1.pdf
- Reglamento de Personal. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/3119BD70-DFB6-4B8C-BC17-3019CC1D0E21/140182/Staff_Regulations_120704EN.pdf

- Reglamento del Personal de la Corte Penal Internacional. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/56F9B14B-B682-4D9C-8762-A25B944FA214/140112/ICCASP43final_Spanish.pdf
- Reglamento Financiero. Extraído el 24 de mayo de 2011, desde: <http://www.icc-cpi.int/NR/rdonlyres/D4B6E16A-BD66-46AF-BB43-8D4C3F069786/281202/FRRENG0705.pdf>
- Reglas de Procedimiento y prueba. Extraído el 24 de mayo de 2011, desde: http://www.icc-cpi.int/NR/rdonlyres/F1E0AC1C-A3F3-4A3C-B9A7-B3E8B115E886/140167/Rules_of_procedure_and_Evidence_Spanish.pdf
- Rome Statute of the International Criminal Court. Extraído el 24 de mayo de 2011, desde: <http://www.icc-cpi.int/nr/rdonlyres/0d8024d3-87ea-4e6a-8a27-05b987c38689/0/romestatuteng.pdf>
- ROMERO, J. de D., (2001, octubre 1). Extraído el 29 de marzo de 2011, desde: <http://www.monografias.com/trabajos7/incer/incer.shtml?monosearch>.
- STAMMLER, Rodolfo. Tratado de Filosofía del Derecho. Traducción de W. Roces. Editorial Reus, Madrid, 1930, núm. 47, pág 117. Citado en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>
- VON IHERING, Rudolf. La lucha por el derecho. Editorial Bibliográfica Omeba, Buenos Aires. Citado en: IRIARTE, C.M., (2008, febrero 17). Definiciones e importancia del Derecho. Extraído el 26 de marzo de 2011, desde: <http://definicionesderecho.blogspot.com/>